



Escuela  
Politécnica  
Superior

# Auditoría TI en la Asociación APSA



Grado en Ingeniería Informática

## Trabajo Fin de Grado

Autor:

Paula González Mataix

Tutor/es:

José Vicente Berná Martínez

Septiembre 2018



Universitat d'Alacant  
Universidad de Alicante

## Resumen

En el presente Trabajo de Fin de Grado se ha creado una metodología de análisis TI (Tecnologías de la Información) mediante la cual se ha establecido una serie de herramientas y procesos para generar una auditoría TI, creando lo que se denomina Plan Auditor. Así como también, se ha llevado a cabo dicho Plan Auditor para realizar una auditoría TI en una empresa real, la Asociación APSA.

La Asociación APSA en estos momentos desarrolla un importante proceso de digitalización de sus servicios y generación de otros nuevos que le permitan mejorar y posicionarse en el sector, por lo que les surge la necesidad de realizar una Auditoría TI y ver cuál es el estado actual en cuanto a la gestión y uso de la TI, razón por la que surge la realización de este Trabajo de Fin de Grado.

Como había una gran falta de conocimiento con respecto a cómo realizar una Auditoría TI, se ha tenido que realizar un estudio sobre Auditorías TI y como realizarlas para poder conocer suficiente sobre este aspecto y poder llegar a la creación del Plan Auditor, que se ha dividido en cuatro fases:

- **Análisis:** en esta fase se identifica el origen o necesidad de la auditoría, se determinan los objetivos y se conoce y estudia la empresa en general.
- **Planificación:** en esta fase se determinan los puntos de la empresa a ser evaluados respecto a la TI después del análisis inicial, se identifican y seleccionan los métodos, herramientas, instrumentos y procedimientos necesarios, y se elaboran los planes y programas para la auditoría junto la asignación de recursos.
- **Ejecución:** fase en la que se llevan a cabo las actividades de recopilación de información mediante las herramientas establecidas, hasta encontrar el punto de satisfacción por las partes implicadas.
- **Dictamen:** fase final en la que, a partir de la información obtenida, se emiten las recomendaciones para la empresa para proporcionarles una mejora en el alineamiento entre empresa y TI a la vez que intentar asegurar el buen gobierno y gestión TI.

Para poder aplicar el Plan Auditor y realizar la Auditoría TI en la Asociación APSA, se han hecho servir dos herramientas: la creación de un cuestionario con preguntas acerca de las áreas que se pretende evaluar y el uso de la Cascada de Metas de COBIT para mejorar el alineamiento entre el negocio y la TI, pudiendo obtener así qué procesos debería tener ésta asociación para su correcto funcionamiento.

Finalmente, y después de la ejecución de la auditoría en la asociación, se ha obtenido un dictamen que será entregado a ésta donde se realizan una serie de recomendaciones sobre cómo mejorar algunos aspectos de las áreas evaluadas, y la explicación sobre cuáles son los procesos que deberían tener, que actividades deberían hacer para implantar estos procesos y cuáles podrían ser las métricas para evaluar el correcto cumplimiento del proceso.

## Motivación y objetivos

Dentro del itinerario de Tecnologías de la Información, de la carrera de Ingeniería Informática, se encuentra la asignatura Gestión y Gobierno de las Tecnologías de la Información que cursé el año académico pasado y que me sirvió de base para poder empezar este trabajo de fin de grado.

En la asignatura Gestión y Gobierno de las Tecnologías de la Información se ve, aunque, por falta de tiempo, de manera muy general, algunos de los principales marcos, estándares y frameworks que utilizan las organizaciones para Gobernar y Gestionar la TI como, por ejemplo, ITIL v3, COBIT 5 o la ISO 38500, así como entender y aprender que función tiene la figura del CIO y la presencia en el comité ejecutivo de la empresa. Aprendimos algunas de las competencias que tiene que tener un Gobernante TI, como tener la capacidad para comprender el entorno de una organización y sus necesidades en el ámbito de las tecnologías de la información y las comunicaciones o algunas competencias de un Gestor TI como son, capacidad para seleccionar, diseñar, desplegar, integrar, evaluar, construir, gestionar, explotar y mantener las tecnologías de hardware, software y redes, dentro de los parámetros de coste y calidad adecuados o capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos. Como también vimos en la asignatura actualmente la TI juega un papel importante en el mundo de la empresa ya que vivimos rodeados de tecnología, por eso el Gobierno TI se encarga de que la TI esté alineada con la estrategia de negocio, de que los servicios y funciones de TI se proporcionan con el máximo valor posible o de la forma más eficiente y de que todos los riesgos relacionados con TI son conocidos y administrados y los recursos de TI están seguros, mientras que la Gestión TI se encarga de proporcionar una adecuada gestión de la calidad, de aumentar la eficiencia, de alinear los procesos de negocio y la infraestructura TI, de reducir los riesgos asociados a los Servicios TI y de generar negocio. Finalmente, vimos que en la parte de Gobierno está el área de cómo dirigir la TI, que suele llamarse auditorías que es el proceso de controlar, de decidir, de establecer que es correcto y que no es correcto, donde algunos marcos como puede ser COSO son especialistas.

Después de cursar la citada asignatura, contacté con el profesor de esta para proponerle que fuera mi tutor para el trabajo de fin de grado. Después de que él aceptara, me propuso un proyecto que me pareció de lo más interesante que estaba relacionado con mis expectativas de trabajo futuro, ya que me gustaría trabajar de algo relacionado con la Gestión y Gobierno de las Tecnologías de la Información o con la Gestión de Proyectos Informáticos. Su propuesta era realizar el trabajo de fin de grado en una asociación de Alicante llamada APSA que se habían puesto en contacto con él y con la Universidad de Alicante para realizar un proyecto TI en el cual, uno de los primeros pasos debía ser una auditoría TI de cara a mejorar la situación de la empresa relacionada con las tecnologías de la información.

Como ya he comentado en el último párrafo, me parece una idea muy interesante, pero al mismo tiempo me parece de una gran responsabilidad ya que se va a realizar una auditoría real, en una empresa real, y esta depende de los resultados que obtenga en este trabajo. Y aunque pueda ser un trabajo costoso o difícil estoy muy ilusionada y confío en que salga bien.

Estoy muy motivada en este proyecto primero por la confianza que ha depositado el tutor en mí y después por poder seguir aprendiendo sobre este tema que tanto me interesa.

## Agradecimientos

A mi madre, por ser mi apoyo constante tanto en estos años de carrera como en todos los momentos de mi vida y por ayudarme a levantarme siempre que caigo.

A mi hermano por hacer mis días más felices.

A mi tutor, por toda la inmensa paciencia que ha tenido conmigo durante la realización de este TFG y por ayudarme y darme consejos en la realización de este TFG y otros aspectos de la vida.

A mis amigas y amigos por entender mis ausencias durante este tiempo.

A todos y cada uno de los compañeros que me han ayudado durante este tiempo, porque sin ellos sería incapaz de estar ahora mismo donde estoy.

## Citas

*“Que els núvols no t’impedisquen veure el sol, el sol sempre ix”*

# Índice de contenido

<b>Resumen .....</b>	<b>2</b>
<b>Motivación y objetivos.....</b>	<b>4</b>
<b>Agradecimientos .....</b>	<b>6</b>
<b>Citas.....</b>	<b>7</b>
<b>Índice de contenido .....</b>	<b>8</b>
<b>Índice de ilustraciones.....</b>	<b>11</b>
<b>Índice de tablas .....</b>	<b>13</b>
<b>1.- Introducción .....</b>	<b>14</b>
1.1.    Problemas en las PYME's .....	16
1.2.    Auditoría TI .....	17
1.3.    Caso concreto de estudio: APSA.....	18
<b>2.- Estudio de viabilidad .....</b>	<b>21</b>
2.1. Análisis DAFO .....	21
2.2. Análisis de riesgos .....	22
<b>3.- Planificación .....</b>	<b>25</b>
<b>4.- Estado del arte: Gestión de la TI en las empresas .....</b>	<b>26</b>
4.1. COBIT 5 y ISACA .....	27
4.2. ITIL.....	34
4.3. ISO 38500 .....	43
4.4. Conclusión .....	45
<b>5.- Estado del arte: Auditorías y como realizarlas .....</b>	<b>47</b>
5.1. Guía para realizar una auditoría informática paso a paso.....	48
5.2. Auditoría Informática Planificación .....	49



<b>5.3. Metodología para realizar una auditoría .....</b>	<b>52</b>
5.3.1. Etapa de Planeación de la Auditoría .....	52
5.3.2. Etapa de Ejecución de la Auditoría .....	55
5.3.3. Etapa de Dictamen de la Auditoría .....	55
<b>5.4. Pasos para realizar una auditoría en sistemas informáticos .....</b>	<b>57</b>
<b>5.5. Procedimientos para la captura de información en la auditoría informática .....</b>	<b>60</b>
<b>5.6. Auditoría de Tecnologías y Sistemas de Información .....</b>	<b>63</b>
5.6.1 Auditoría Informática .....	63
5.6.2 El Plan Auditor Informático .....	65
5.6.3. Contrato de Auditoría .....	66
5.6.4 Principales áreas de la auditoría informática .....	66
<b>5.7. Conclusiones .....</b>	<b>67</b>
<b>6.- Estado del arte: Inventario .....</b>	<b>68</b>
6.1. Software de código abierto para la gestión del inventario .....	68
6.2. Conclusión .....	73
<b>7.- Antecedentes .....</b>	<b>75</b>
<b>8.- Objetivos .....</b>	<b>83</b>
<b>9.- Plan auditor .....</b>	<b>84</b>
9.1.- Etapa de análisis .....	84
9.2.- Etapa de planificación .....	86
9.3.- Etapa de ejecución .....	88
9.4.- Etapa de dictamen .....	89
<b>10.- Auditoría (resultados) .....</b>	<b>91</b>
10.1. – Etapa de análisis .....	91
10.2. – Etapa de planificación .....	114

<b>10.3.- Etapa de ejecución.....</b>	<b>118</b>
<b>10.4.- Etapa de dictamen.....</b>	<b>136</b>
10.4.1. Proceso Asegurar la Entrega de Beneficios.....	136
10.4.2 Proceso Gestionar el Portafolio.....	140
10.4.3 Proceso Gestionar los Recursos Humanos .....	145
10.4.4 Proceso Gestionar la Calidad.....	152
10.4.5 Proceso de Gestión de Programas y Proyectos .....	157
10.4.6 Métricas TI.....	172
10.4.7. Acciones a corto plazo .....	173
<b>11.- Resultados .....</b>	<b>178</b>
<b>12.- Conclusiones y trabajo futuro .....</b>	<b>180</b>
<b>Glosario .....</b>	<b>181</b>
<b>Referencias, bibliografía y apéndices .....</b>	<b>183</b>
<b>Apéndice I .....</b>	<b>185</b>
<b>Apéndice II .....</b>	<b>194</b>

# Índice de ilustraciones

Ilustración 1. Estructuración de servicios en APSA según etapas vitales del individuo.	19
Ilustración 2. Catalizadores de COBIT .....	29
Ilustración 3. Cascada de metas de COBIT 5 .....	32
Ilustración 4. Ciclo de Vida del Servicio .....	37
Ilustración 5. Etapas de una auditoría. ....	57
Ilustración 6. Página principal del Inventario .....	69
Ilustración 7. Trazabilidad del Inventario .....	69
Ilustración 8. Vista I del Inventario .....	70
Ilustración 9. Vista II del Inventario .....	70
Ilustración 10. Página del inventario .....	71
Ilustración 11. Página del inventario .....	71
Ilustración 12. Página del inventario .....	72
Ilustración 13. Página del inventario .....	73
Ilustración 14. Organigrama APSA .....	92
Ilustración 15. Departamentos-Servicios-Áreas APSA .....	93
Ilustración 16. Arquitectura de red de comunicación .....	111
Ilustración 17. Arquitectura de Red en la nube.....	113
Ilustración 18. Procesos de TI Empresarial .....	135
Ilustración 19. Cascada de metas APSA .....	173

Ilustración 20. Objetivos de la empresa.....	185
Ilustración 21. Objetivos de las TI .....	186
Ilustración 22. Muestra de Métricas de Metas Corporativas .....	187
Ilustración 23. Ejemplo de Métricas de Metas TI .....	188
Ilustración 24. Mapeo entre las Metas Corporativas y las Preguntas del Gobierno y la Gestión.....	190
Ilustración 25. Mapeo entre las Metas Corporativas y Metas TI .....	191
Ilustración 26. Mapeo entre las Metas Relacionadas con la TI y los Procesos .....	193

## Índice de tablas

Tabla 1. Análisis DAFO.....	22
Tabla 2. Análisis de riesgos.....	23
Tabla 3. Planificación temporal TFG .....	25
Tabla 4. Perfiles de los auditores .....	50
Tabla 5. Equipos APSA.....	110
Tabla 6. Mapeo entre Metas Corporativas y Metas TI .....	131
Tabla 7. Mapeo entre Metas Relacionadas con TI y Procesos .....	134

# 1.- Introducción

Nos movemos en una sociedad tecnológica, lo que significa que la tecnología de la información está presente actualmente en todas y cada una de las empresas en mayor o menor medida y esto, aunque es beneficioso para las empresas puede suponer un problema, ya que la TI avanza de manera muy rápida.

Por lo general, las empresas nacen y poco a poco van creciendo, por lo que pueden ocurrir dos tipos de situaciones: la primera es que la empresa se creara hace mucho tiempo y que en el momento de su creación no necesitaran nada de TI para su funcionamiento y que por adaptación al medio hayan tenido que implantarla en su empresa, con todo lo que conlleva tener que hacerlo, mientras que la segunda situación es que la empresa sea más actual y que en el momento de su creación ya implantara TI en su negocio. Sea cual sea la situación de la empresa, el mayor problema que presenta es que, aparte de lo rápido que avanza la TI y la problemática que esto supone para la adaptación de la empresa a las nuevas tecnologías, la empresa nace y va creciendo y la TI se va adaptando a ella sin ningún planteamiento específico, es decir, se va solucionando los problemas que puedan ocurrir con esta como van ocurriendo, parcheando lo que haga falta para que la empresa pueda seguir funcionando y esto genera un gran problema a largo plazo.

Otro de los problemas a los que se tiene que enfrentar una empresa, es que a no ser que sea una empresa relacionada directamente con la TI, no suele existir dentro de ella una figura responsable de la TI, con lo que externalizan los servicios a otras empresas que se encargan de proporcionarlos y dependen de estos para que su negocio funcione, o bien las funciones de desarrollo, implantación y tecnificación en general las asumen personas no cualificadas (a veces simplemente aficionados a la tecnología) y sin las competencias necesarias.

Finalmente, estas situaciones lo que provocan es el que la TI no esté alineada con el negocio, ya que muchas veces la TI no se incluye como uno de los apartados del plan estratégico de la empresa por lo que es mucho más difícil ver si las mejoras que se van

haciendo en la TI apoyan algunos de los objetivos de la empresa o cómo contribuyen efectivamente en la creación de valor.

Por todo lo comentado anteriormente, y como pudimos aprender en la asignatura Gestión y Gobierno de las Tecnologías de la Información, donde vemos, aunque de manera muy superficial por falta de tiempo, algunos de los principales marcos, estándares y frameworks que utilizan las organizaciones para Gobernar y Gestionar la TI que podrían solucionar el mayor problema que es el de ir parcheando, así como también sabemos que es importante que en el Plan Estratégico de la empresa, se tenga en cuenta la TI, para que así se asegure que todas las decisiones que se tomen con respecto a esta estén alineadas con la estrategia de la empresa. Otra de las cosas que vimos y que solucionaría el problema de tener que externalizar los servicios es tener una persona encargada de gestionar la TI, llamada CIO.

El CIO (Chief Information Officer) es un título de trabajo comúnmente otorgado al más alto ejecutivo de una empresa responsable de la tecnología de la información y los sistemas informáticos que respaldan los objetivos de la empresa. Típicamente, el CIO reporta directamente al director ejecutivo, pero también puede informar al director de operaciones o al director financiero.

La función del CIO o Gerente de Sistemas, es la de orientar los sistemas de información con los planes de crecimiento y la estrategia de la empresa, con el fin de que esta pueda conseguir los objetivos planteados. [1]

Algunas de las principales características que debe cumplir un CIO son las siguientes:

- Capacidad de planificación para poder visualizar el entorno que necesitará en el plazo fijado en los objetivos.
- Organización para saber gestionar toda la documentación (informes, presupuestos, etc.)
- Coordinación para gestionar al personal interno o externo que esté a su cargo.
- Liderazgo para el trato con proveedores y personal interno.
- Control para poder cumplir los plazos pactados.

- Perfil orientado hacia los negocios para resolver los problemas de la empresa con la tecnología a su alcance.
- Capacidad de gestión financiera para estudiar los costos.
- Habilidades comunicativas para poder transmitir fácilmente el complejo lenguaje técnico.

## 1.1. Problemas en las PYME's

Las pymes necesitan incorporar tecnología a sus estrategias de negocio para poder ser más productivas y aumentar su grado de eficiencia y esta incorporación aumenta cada vez más. En 2015, un 99,2% de las pymes y grandes empresas españolas y un 74,1% de las microempresas disponían de lo que se puede considerar tecnología básica, es decir, un PC [2], además la mayoría de pymes y grandes empresas disponen también de conexión a la red y de algunos dispositivos móviles que permitan cierta interconexión en algunos procesos.

Con estos números nos podemos percatar que la demanda de tecnologías de información por parte de las pymes es considerable y la mayoría se empiezan a dar cuenta, o ya se han dado cuenta, de que el uso de las tecnologías de información contribuye a mejorar los procesos del negocio.

Sin embargo, cabe mencionar que existen obstáculos o barreras que intervienen en la adquisición e implantación de tecnologías de información dentro de las pymes.

Existen 4 barreras principales que a lo largo de los años han impedido que las pymes logren su propio cambio, innovación y modernización y son las siguientes [3]:

1. *Resistencia al cambio* por diferentes aspectos, como son, el temor por parte de los trabajadores al uso de alguna nueva tecnología, los errores en el uso de la nueva tecnología, el cambio de cultura y comportamiento, es decir, dejar lo que se estaba haciendo hasta ahora para incorporar nuevas prácticas y la escasa participación de los usuarios finales (trabajadores o clientes) en el levantamiento de los requerimientos, diseño y desarrollo de las aplicaciones.



2. *Mala definición de requerimientos* por diferentes aspectos como, la falta de compromiso de los involucrados (gerencias, clientes y/o proveedores), la escasa coordinación entre los niveles jerárquicos de la empresa y la falta de experiencia en el desarrollo e implementación de proyectos de esta índole.
3. *Hardware y software* donde muchas de las pymes no cuentan con un soporte técnico eficiente.
4. *Dependencia de los proveedores de tecnología*

Además de todos los factores comentados anteriormente en la implantación de la TI, tenemos las cuestiones que surgen una vez implantada. Como hemos comentado en el apartado anterior, la TI avanza muy rápidamente y las pymes no suelen tener ninguna estrategia clara de cómo abordar los problemas, simplemente los van solucionando como pueden cuando ocurren, comúnmente el llamado “apaga fuegos”, así como tampoco suelen disponer de un gestor o encargado de TI. Por todo ello una vez que la tecnología supera a la empresa, realizar una Auditoría TI suele ser la opción idónea, para poder ayudar a la empresa a mejorar esta situación.

## 1.2. Auditoría TI

Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos [4].

La Auditoría de las Tecnologías de Información, mejor conocida como “Auditoría TI” o “Auditoría Informática”, es una actividad de control que comprende la evaluación de las TI, así como de la seguridad informática, dentro de una organización [5]. Está basada en buenas prácticas y normas nacionales e internacionales, que son utilizadas para revisar y calificar el diseño, desempeño y cumplimiento de los controles implementados en el ambiente TI.

Permite contar con una evaluación objetiva e independiente respecto a los procesos, servicios, aplicaciones, infraestructura e información, identificando los principales riesgos de negocio relacionados con TI, resultado de posibles debilidades de control.

Los mecanismos de control de la auditoría pueden clasificarse en directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

Los principales beneficios de una auditoría TI son:

- **Verificar** que los servicios de TI se encuentran al nivel que la organización necesita para habilitar, potenciar y soportar de manera efectiva y eficiente sus funciones sustantivas.
- **Determinar** si el ambiente de control en TI, cumple con las regulaciones y requerimientos normativos.
- Contar con las recomendaciones necesarias para **mitigar** posibles riesgos que pongan en peligro a los activos de información y a la continuidad del negocio.

Otros beneficios de una auditoría TI son: mejora la imagen pública, genera confianza en los usuarios sobre la seguridad y control de los servicios de TI, realiza un control de la inversión en un entorno de TI.

La auditoría TI sirve para mejorar ciertas características en la empresa como pueden ser: desempeño, fiabilidad, eficacia, rentabilidad, seguridad y privacidad.

Finalmente, comentar que se puede desarrollar en alguna de las siguientes áreas o en alguna combinación de ellas: gobierno corporativo, administración del ciclo de vida de los sistemas, servicios de entrega y soporte, protección y seguridad y planes de continuidad y recuperación de desastres.

### 1.3. Caso concreto de estudio: APSA

En este TFG, además de realizar un estudio teórico, también contaremos con una propuesta concreta de auditoría a una asociación real. La asociación donde vamos a realizar la Auditoría TI es la Asociación APSA.

APSA es una asociación sin ánimo de lucro creada en el año 1962 y declarada de utilidad pública en 1970. Su misión es mejorar la calidad de vida de las personas con discapacidad o riesgo de presentarla, y la de sus familias o tutores legales.

El grupo APSA está compuesto por la Asociación APSA y sus tres centros especiales de empleo: Avícola Aguamarga, Limencop y Terramar. Atiende a alrededor de 2000 personas al año en diversas localidades de la provincia de Alicante. Para ello, cuenta con más de 350 trabajadores, de los cuales más de 200 son personas con discapacidad.

APSA ofrece recursos para satisfacer las necesidades de apoyo de sus socios, a lo largo de todo su ciclo vital. Por este motivo, a lo largo de sus más de 50 años de historia ha desarrollado diversos centros y servicios.

Ofrecen servicios en la etapa educativa, la etapa de transición a la vida adulta, la etapa de vida adulta, o la etapa de tercera edad, como puede observarse en la figura a continuación:

De 0 a 16 años	De 16 a 26 años	De 26 a 65 años	A partir de 65 años
<b>ETAPA EDUCATIVA</b>	<b>TRANSICIÓN A LA VIDA ADULTA</b>	<b>VIDA ADULTA</b>	<b>TERCERA EDAD</b>
<ul style="list-style-type: none"> <li>- Centro de Desarrollo Infantil y Atención Temprana</li> <li>- Centro de Recursos y Apoyo Escolar</li> <li>- Ocio y deporte</li> <li>- Respiro familiar</li> <li>- Apoyo Psicológico</li> <li>- Formación en nuevas tecnologías</li> <li>- Actividades artísticas</li> <li>- Formación a familias</li> <li>- Trabajo social</li> <li>- Unidad Volante de Apoyo a la Dependencia</li> <li>- Servicio de apoyo educativo</li> </ul>	<ul style="list-style-type: none"> <li>- Centro Camí Obert</li> <li>- Ocio y deporte</li> <li>- Respiro familiar</li> <li>- Formación en nuevas tecnologías</li> <li>- Unidad Volante de Apoyo a la Dependencia</li> <li>- Trabajo social</li> <li>- Apoyo Psicológico</li> <li>- Actividades Artísticas</li> <li>- Vivienda</li> </ul>	<ul style="list-style-type: none"> <li>- Centro de Orientación y Formación</li> <li>- Asesoramiento Laboral</li> <li>- Centro Ocupacional Terramar</li> <li>- Centros Especiales de Empleo</li> <li>- Ocio y deporte</li> <li>- Respiro familiar</li> <li>- Unidad Volante de Apoyo a la Dependencia</li> <li>- Apoyo Psicológico</li> <li>- Formación a familias</li> <li>- Trabajo social</li> <li>- Actividades Artísticas</li> <li>- Viviendas</li> <li>- Psiquiátrico Penitenciario</li> </ul>	<ul style="list-style-type: none"> <li>- Envejecimiento saludable</li> <li>- Ocio y deporte</li> <li>- Unidad Volante de Apoyo a la Dependencia</li> <li>- Trabajo social</li> <li>- Apoyo Psicológico</li> <li>- Actividades Artísticas</li> </ul>

Ilustración 1. Estructuración de servicios en APSA según etapas vitales del individuo.

Esta asociación en 2017 ha logrado el apoyo de Aguas de Alicante a través de una Cátedra de Inclusión dirigida por el Vicerrectorado de Responsabilidad Social, Inclusión e Igualdad, a través de la cual va a realizar un importante esfuerzo de innovación TI para ofrecer nuevos servicios y mejorar sus actuales procesos empresariales. Este proyecto de innovación persigue la mejora y crecimiento en la oferta de servicios a sus asociados.

Tras lo comentado anteriormente, establecemos que el objetivo principal de este Trabajo de Fin de Grado será abordar las cuestiones relativas a la realización de una Auditoría TI. Para validar nuestro estudio vamos a aprovechar el vínculo que la Universidad de Alicante posee con la asociación APSA a través de la Cátedra de Inclusión, para concretar esta auditoría en el proceso de innovación TI real de la Asociación APSA.

La Asociación APSA a través de esta Cátedra pretende realizar un cambio en su forma de trabajar pasando de la manera tradicional a una inclusión fuerte de la TI. Este cambio de forma de trabajar, tendiendo hacia la TI es la que obliga y justifica el realizar una auditoría TI, ya que la empresa va a hacer una fuerte inversión tanto organizacional como económica para apostar por la oferta de servicios digitales, que tengan un mayor alcance, un mayor impacto y aumenten la cadena de valor de la asociación. Antes de crear nuevos servicios, es necesario analizar los actuales, la TI desplegada, y alinear los servicios existentes junto con los nuevos objetivos de negocio y la TI que tendremos que crear.

## 2.- Estudio de viabilidad

En este apartado, vamos a realizar un estudio de viabilidad para entender como nos encontramos con respecto a lo que queremos realizar, así como darnos cuenta de si realmente vamos a poder realizar el trabajo que nos hemos propuesto. Para ello vamos a hacer un análisis DAFO y un análisis de riesgos.

### 2.1. Análisis DAFO

El análisis DAFO es una herramienta utilizada para examinar las Debilidades, Amenazas, Fortalezas y Oportunidades de una empresa o proyecto. En nuestro caso, se trata de analizar las características internas del proyecto que vamos a realizar, así como las más propias y la situación externa.

El análisis DAFO se realiza desde dos enfoques:

- Interno:

- Fortalezas: Se trata de las ventajas que tiene el proyecto, aquello que lo hace mejor que los otros.
- Debilidades: Hacen referencia a aquello que puede ser mejorado y aquello que se debería evitar.

- Externo:

- Oportunidades: son aquellos factores positivos que se generan en el entorno y que, una vez identificados, pueden ser aprovechados.
- Amenazas: son situaciones negativas, externas al programa o proyecto, que pueden atentar contra éste por lo que, llegado al caso, puede ser necesario diseñar una estrategia adecuada para poder sortearlas.

Análisis DAFO	Fortalezas	Debilidades
Análisis interno	<ul style="list-style-type: none"> <li>- Constancia</li> <li>- Ganas de aprender sobre Auditoría TI</li> <li>- Gran motivación por la realización de este proyecto</li> </ul>	<ul style="list-style-type: none"> <li>- Falta de conocimiento sobre Auditoría TI</li> <li>- Falta de experiencia en la realización de una Auditoría TI</li> </ul>
	Oportunidades	Amenazas
Análisis externo	<ul style="list-style-type: none"> <li>- Gran cantidad de información en internet</li> <li>- Posibilidad de aprender cómo se debe realizar una auditoría TI</li> <li>- Posibilidad de aplicar los conocimientos aprendidos en un caso real</li> </ul>	<ul style="list-style-type: none"> <li>- Falta de tiempo por tener otras asignaturas</li> </ul>

Tabla 1. Análisis DAFO

## 2.2. Análisis de riesgos

Un análisis de riesgos es el estudio de las causas de las posibles amenazas y probables eventos no deseados, así como los daños y consecuencias que éstas puedan producir. En nuestro caso, tenemos que ver los problemas que pueden ocurrir durante el proyecto y el grado de gravedad para la realización del mismo.

Riesgo	Probabilidad	Impacto
Desconocimiento de auditoría TI	Alta	Tolerable
Enfermar durante el curso	Alta	Serio
Tener más trabajo debido a asignaturas	Alta	Tolerable/Serio
Que se rompa el ordenador	Baja	Catastrófico
Tener un accidente con el coche	Media	Catastrófico
La empresa pida más cosas	Alta	Serio
Planificación demasiado optimista	Alta	Tolerable/Serio

Que nieve y no haya luz en varios días	Baja	Tolerable
--	------	-----------

*Tabla 2. Análisis de riesgos*

- El desconocimiento de cómo realizar una Auditoría TI tiene una probabilidad alta de ocurrir y tendría un impacto tolerable ya que se podría solucionar con el tiempo ya que se puede aprender sobre esto, por lo tanto, la solución sería investigar y buscar información para aprender sobre ello.
- El riesgo de enfermarse durante el curso tiene una probabilidad alta ya que, se puede enfermarse por múltiples cosas y de múltiples maneras, como pueda ser coger un resfriado, coger una gripe, padecer una gastroenteritis, aunque la más probable es la de coger un resfriado y esto puede suceder varias veces durante el curso por lo que el impacto podría llegar a ser serio si llega a impedir durante bastante tiempo el curso normal de la realización del TFG. Es difícil prever esto, pero se podría combatir planificando el tiempo teniendo en cuenta que esto puede ocurrir.
- La probabilidad de tener más trabajo debido a asignaturas es alta ya que, al tener más asignaturas en la carrera, aparte del TFG, en diversas épocas se va a tener más trabajo que van a impedir que se pueda seguir realizando el TFG porque se va a tener que realizar el trabajo relacionado con las asignaturas de la carrera. Esto se puede solucionar como el riesgo anterior, planificando el tiempo de realización teniendo en cuenta que esto puede ocurrir y más probablemente en los meses de octubre, diciembre, marzo y mayo.
- La probabilidad de que se rompa el ordenador de trabajo es baja porque es un ordenador bastante nuevo y no debería romperse, pero podría suceder y en caso de suceder sería catastrófico, porque perderíamos el trabajo y la forma más cómoda de seguir realizándolo. Este problema se podría solucionar haciendo copia de cada cambio que se haga y teniendo también un ordenador de repuesto.
- Tener un accidente con el coche tiene una probabilidad de ocurrir media ya que se utiliza el coche para ir a la universidad y puede ocurrir un accidente por

múltiples causas y tendría un efecto catastrófico porque no se podría seguir el curso planificado del proyecto. Esto se podría solucionar teniendo en cuenta que puede ocurrir esto en la planificación del proyecto.

- Que la empresa pida más cosas a lo largo de la realización del proyecto tiene una probabilidad alta y podría tener un riesgo serio ya que haría que la planificación no se cumpla. Se podría solucionar dejando claro desde el principio que es lo que se quiere realizar.
- Para solucionar el problema de una planificación demasiado optimista que tiene una probabilidad de ocurrir alta y tendría un efecto de tolerable a serio, se podría intentar ser consciente de nuestras limitaciones y planificar de manera más real teniendo en cuenta todo lo que puede fallar a nuestro alrededor e impedir que se cumplan los tiempos.
- Que nieve y no haya luz en varios días va a impedir posiblemente que podamos trabajar durante ese tiempo, lo que tiene una probabilidad baja de ocurrir y además el impacto sería tolerable ya que podríamos seguir con el TFG una vez volviera la luz. Además, esto se puede prever teniendo en cuenta que hay una pequeña probabilidad de que ocurra, al hacer la planificación.



### 3.- Planificación

En este apartado se va a realizar una planificación estimada sobre cada uno de los puntos y apartados que vamos a seguir en la realización del TFG.

<i>Contenido</i>	<i>Tiempo</i>
Visitas a APSA	12 horas
Redacción motivación y justificación	6 horas
Redacción introducción	10 horas
Redacción estudio de viabilidad	5 horas
Redacción planificación	1 hora
Búsqueda de información sobre los problemas en la gestión de la TI	16 horas
Búsqueda de información sobre auditoría TI	42 horas
Búsqueda de información sobre programas para inventario	3 horas
Redacción estado del arte	70 horas
Redacción apartado antecedentes	26 horas
Redacción de objetivos	1 hora
Búsqueda de información plan auditor	6 horas
Redacción plan auditor	18 horas
Redacción auditoría	60 horas
Redacción resultados	8 horas
Redacción conclusión y trabajo futuro	6 horas
Resto de detalles de redacción	10 horas

*Tabla 3. Planificación temporal TFG*

## 4.- Estado del arte: Gestión de la TI en las empresas

Como ya hemos comentado anteriormente, las empresas suelen tener varios problemas para gestionar la TI en sus empresas y algunos de los problemas a los que se tienen que enfrentar son:

- Cuando crece una empresa los problemas que tiene con respecto a la TI se van solucionando como se puede sin tener ningún plan de actuación para poder solucionar los problemas de manera efectiva.
- Muchas organizaciones, en particular las pequeñas y medianas empresas, a menudo harán uso de los recursos internos para realizar el mantenimiento de TI para lo cual la TI es un “pasatiempo”. A corto plazo, esta puede ser una forma rentable de administrar la TI, pero generalmente producirá problemas, ya que no va a poder brindar el mismo nivel de servicio que un profesional capacitado para administrar la TI.
- La TI no está alineada con el plan estratégico de la empresa por lo que no se sabe si los cambios o implementaciones que se hacen con respecto a la TI contribuyen a la creación de valor de la empresa.
- Los sistemas de TI modernos requieren atención constante para mantenerlos funcionando al 100% y si no es así se comportarán mal y se necesitará más tiempo para solucionar los problemas.
- Los sistemas para la administración de TI cada vez son más complejos, como infraestructuras de la nube o la virtualización de los servidores. Estas tecnologías tienen la garantía de mejorar las operaciones comerciales y ayudar al crecimiento del negocio, pero también producen estrés para quien se encargue de la administración de la TI.

Como las empresas crecen sin un plan establecido, es decir, no tienen una organización ni una serie de elementos que asegure una correcta gestión y gobierno de la TI (el gobierno marca las directrices que debe llevar el gestor a cabo, y el gestor marca como

llevan a cabo las directrices) han surgido diversos marcos, frameworks y estándares, así como asociaciones que ayudan a saber cómo solucionar los problemas anteriores.

## 4.1. COBIT 5 y ISACA

La primera asociación que nos interesa y que tiene relación con el marco de COBIT 5 es ISACA. Vamos a explicar brevemente que es ISACA para poder entender porque nos va a servir:

ISACA (Information Systems Audit and Control Association) es un líder global proveedor de conocimiento, certificaciones, comunidad, promoción y educación sobre aseguramiento y seguridad de sistemas de información (SSII), gobierno empresarial y gestión de TI y riesgo relacionado con TI y cumplimiento. Fundada en 1969, ISACA, independiente y sin ánimo de lucro, celebra conferencias internacionales, publica el ISACA Journal y desarrolla estándares internacionales de control y auditoría de SSII (Sistemas de Información), que ayudan a sus miembros a asegurar la confianza en, y aportar valor desde, los sistemas de información. También avanza y avala habilidades y conocimientos en TI mediante los globalmente reconocidos certificados (CISA) Certified Information Systems Auditor, (CISM) Certified Information Security Manager, (CGEIT) Certified in the Governance of Enterprise IT y (CRISC) Certified in Risk and Information Systems Control . [6]

ISACA actualiza continuamente el COBIT (COBIT es un framework de ISACA), el cuál ayuda a los profesionales de TI y líderes de las organizaciones a llevar a cabo sus responsabilidades en la gestión y gobierno de TI, particularmente en las áreas de aseguramiento, seguridad, riesgo y control y proporcionar valor al negocio.

Después de ver brevemente que es ISACA y porque se relaciona con COBIT vamos a explicar el framework COBIT 5.

COBIT 5 ayuda a las Organizaciones a crear un valor óptimo a partir de la TI, al mantener un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos, así como también, permite que las tecnologías de la

información y relacionadas se gobiernen y administren de una manera holística a nivel de toda la Organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios, considerando los intereses relacionados con la TI de las partes interesadas internas y externas.

Los principios y habilitadores de COBIT 5 son genéricos y útiles para las Organizaciones de cualquier tamaño, bien sean comerciales, sin fines de lucro o del sector público, por lo que nos podría resultar útil saber cuáles son estos principios y habilitadores de cara a poder aplicarlos posteriormente a la asociación APSA.

COBIT 5 se basa en cinco principios claves para el gobierno y la gestión de TI empresariales:

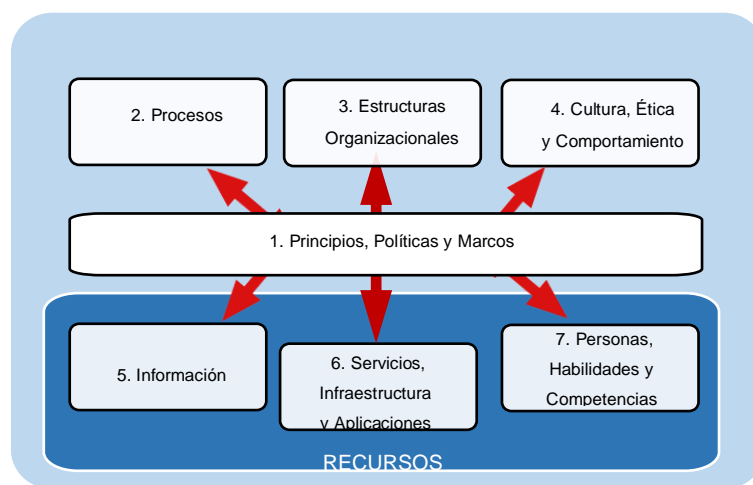
*Principio 1: Satisfacer las Necesidades de las Partes Interesadas* – Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos. Las organizaciones tienen muchas partes interesadas y “crear valor” significa cosas diferentes – a veces conflictivas – para cada una de ellas. COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. El sistema de Gobierno deberá considerar todas las partes interesadas al tomar decisiones con respecto a la evaluación de riesgos, los beneficios y el manejo de recursos ya que, el Gobierno trata de negociar y decidir entre los diversos intereses de beneficio de las diferentes partes interesadas. Finalmente, las necesidades de las Partes Interesadas deben ser transformadas en una estrategia accionable para la organización, por ello, las metas en cascada de COBIT 5 traducen las necesidades de las partes interesadas en metas específicas, accionables y personalizadas dentro del contexto de la organización, de las metas relacionadas con la TI y de las metas habilitadoras.

*Principio 2: Cubrir la Compañía de Forma Integral* - COBIT 5 se concentra en el gobierno y la gestión de la tecnología de la información y relacionadas desde una perspectiva integral a nivel de toda la Organización, lo que significa que integra el gobierno de la TI corporativa en el gobierno corporativo y también cubre todas las funciones y los

procesos dentro de la Organización, es decir, trata la tecnología de la información y relacionadas como activos que necesitan ser manejados como cualquier otro activo.

*Principio 3: Aplicar un Marco de Referencia Único Integrado* - COBIT 5 está alineado con los últimos marcos y normas relevantes usados por las organizaciones por lo que se permite a la Organización utilizar COBIT 5 como integrador macro en el marco de gobierno y gestión.

*Principio 4: Hacer Posible un Enfoque Holístico* – Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores o habilitadores para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo COBIT 5 define siete categorías de catalizadores:



*Ilustración 2. Catalizadores de COBIT*

(Apuntes asignatura GGTI)

1. Principios, Políticas y Marcos – Son los vehículos para traducir el comportamiento deseado en una orientación práctica para la gestión diaria.
2. Procesos – Describen una serie organizada de prácticas y actividades para lograr determinados objetivos y producir una serie de resultados como apoyo al logro de las metas globales relacionadas con la TI.
3. Estructuras Organizacionales – Constituyen las entidades claves para la toma de decisiones en una organización.

4. Cultura, Ética y Comportamiento – De los individuos, así como de la organización.
5. Información – Se encuentra presente en todo el ambiente de cualquier organización.
6. Servicios, Infraestructura y Aplicaciones – Incluyen la infraestructura, la tecnología y las aplicaciones que proporcionan servicios y procesamiento de tecnología de la información a la organización.
7. Personas, Habilidades y Competencias – Están vinculadas con las personas y son requeridas para completar exitosamente todas las actividades y para tomar las decisiones correctas, así como para llevar a cabo las acciones correctivas.

Para lograr los objetivos principales de la Organización, siempre debe considerarse una serie interconectada de habilitadores.

*Principio 5. Separar el Gobierno de la Gestión* – El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. La visión de COBIT 5 en esta distinción clave entre gobierno y gestión es:

- El Gobierno asegura que se evalúen las necesidades de las partes interesadas, así como las condiciones y opciones, para determinar los objetivos corporativos balanceados acordados a lograr; fijando directivas al establecer prioridades y tomar decisiones; así como monitorear el desempeño, cumplimiento y progreso comparándolos contra las directivas y objetivos fijados. En muchas corporaciones, el gobierno global es responsabilidad del comité de dirección bajo el liderazgo del presidente. Algunas responsabilidades de gobierno específicas se pueden delegar en estructuras organizativas especiales al nivel apropiado, particularmente en las corporaciones más grandes y complejas.
- La Gestión planifica, construye, ejecuta y monitorea las actividades conforme a las directivas fijadas por el ente de Gobierno para lograr las metas empresariales. En muchas empresas, la gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del Director General Ejecutivo (CEO).

Una compañía puede organizar sus procesos como estime conveniente, siempre y cuando queden cubiertos todos los objetivos necesarios de gobierno y administración.

Para terminar de entender COBIT, voy a hablar sobre la cascada de metas que lo que permite es tener un sistema casi mecánico para extraer orientación pertinente a incluir en proyectos específicos de implementación, mejora o aseguramiento. [7]

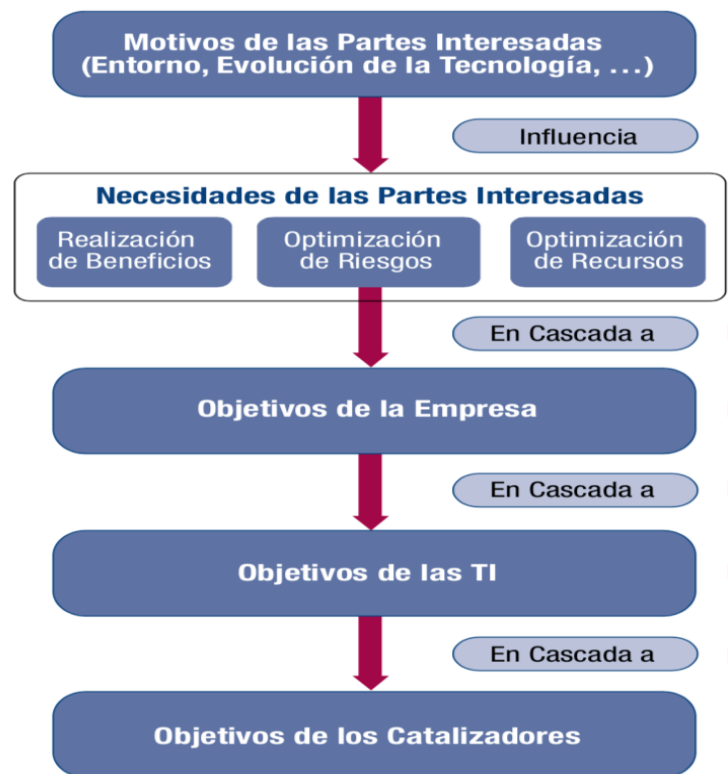
La cascada de metas de COBIT 5 es el mecanismo para traducir las necesidades de las partes interesadas en metas corporativas específicas, practicables y personalizadas, metas de TI y metas de los catalizadores.

En las metas no se distingue tipos de empresa ni tipos de negocio, solo son buenas prácticas que deberían llevarse a cabo. Es solo una orientación, que usa el patrón adopta y adapta que es, tomar los elementos que más se adecúan a nuestras necesidades y adaptarlos para que se acoplen como un guante a sus requerimientos, sistema, etc. Es necesario identificar y relacionar como estas metas se van desarrollando ya que es un proceso reflexivo no automático.

Los pasos a seguir de la cascada de metas son los siguientes:

- Paso 1. Los Motivos de las Partes Interesadas influyen en las Necesidades de las Partes Interesadas
- Paso 2. Las Necesidades de las Partes Interesadas en Cascada hacia Metas Corporativas: Las necesidades de las partes interesadas pueden estar relacionadas con un conjunto de metas genéricas corporativas.
- Paso 3. Metas Corporativas en Cascada hacia Metas TI: El logro de las metas corporativas requiere una serie de resultados TI, representados por las metas relacionadas con TI.
- Paso 4. Metas TI en Cascada hacia Metas de los Catalizadores: Lograr las metas TI requiere la aplicación y uso exitoso de una serie de catalizadores, anteriormente comentados. Para cada catalizador se puede definir un conjunto de metas específicas y relevantes en apoyo a las metas TI.

Los pasos anteriores describen como la cascada de metas permite pasar de las necesidades de las partes interesadas a metas corporativas, de metas corporativas a metas TI y de metas TI a procesos.



*Ilustración 3. Cascada de metas de COBIT 5*

(COBIT 5 – Procesos Catalizadores)

En el apéndice I se puede encontrar como pasar de las necesidades de las partes interesadas a las metas corporativas u objetivos de la empresa y también sus métricas, de las metas corporativas a las metas TI u objetivos de las TI y sus métricas, y finalmente de las metas TI a los procesos u objetivos de los catalizadores.

Para ejecutar una cascada de metas COBIT hay que tener en cuenta que se distingue entre métricas de las metas corporativas, métricas de las metas TI y procesos:

Métricas metas corporativas: son indicadores numéricos que permiten ordenar y saber el grado de cumplimiento de las metas, por lo que hay que saber cuáles son los indicadores para medir el éxito. Junto a cada indicador además de indicar como se mide, hay que decir en que rango es aceptable.

Métricas metas TI: donde en un buen sistema de gestión y gobierno de la TI debería implementarse estos indicadores, pero estos indicadores no te dicen cómo se implementa.



Procesos: son los catalizadores que permiten que una empresa al final haga un buen gobierno, es decir son una serie de prácticas que tienen que ver con las políticas y los procedimientos de la empresa que tienen unas entradas y produce una salida, para ello se define cuáles son las partes interesadas, también cuáles son las metas de proceso que tiene que ver con las metas TI y que al final son metas corporativas.

Las métricas del proceso sirven para poder medir el grado de cumplimiento de las metas de proceso concreto.

Los procesos pueden tener objetivos que tengan que ver con mejorar aspectos internos de la empresa (medir la gestión del rendimiento), con los clientes externos o con la seguridad y accesibilidad (sistema de gestión de las políticas de seguridad respecto a la TI). Cada uno de estos procesos va a tener una gestión basada en su ciclo de vida. Un proceso está en continua revisión.

Para cada proceso se especifica una guía de buenas prácticas que se basan en tres elementos, prácticas, actividades y actividades detalladas. Las prácticas son una serie de líneas de acciones que se deberían llevar a cabo para que ese proceso funcione correctamente (tener en cuenta los empleados, el tipo de productos...). Se dan también unas líneas de actividades concretas que ese proceso tiene que llevar a cabo (ver cuáles son las entradas del proceso, cuáles son las salidas, con que personas están relacionadas...).

Gestión del rendimiento del catalizador: para cada uno se pretende responder a las siguientes preguntas:

- ¿Se atienden las necesidades de las partes interesadas? Y para saberlo hay que saber cuáles son las partes interesadas
- ¿Se atienden los objetivos de los catalizadores? Y hay que saber cuáles son los objetivos
- ¿Se gestiona el ciclo de vida? Para ello se debe establecer un ciclo de vida
- ¿Se aplican buenas prácticas? Para ello hay que tener detalladas las buenas prácticas

Guía de proceso: Cada proceso tiene una guía que te detalla lo que tienes que hacer. Lo

que contienen las guías es: un identificador de proceso, la descripción del proceso, el propósito del proceso, información acerca de las cascadas de metas, te da las métricas del proceso, te da una matriz RACI, te dice todos los que están y de qué manera, información detallada de las prácticas de proceso, cuáles son las guías relacionadas y las entradas y salidas.

Algunos detalles sobre un ejemplo concreto de un proceso: se diferencia entre metas TI y métricas relacionadas, como también entre metas del proceso y métricas relacionadas. Cada proceso tendrá unas métricas propias. Después aparece la matriz RACI indicando todos los agentes a los que les puede resultar interesante para cada métrica; el responsable de las acciones es el que hace que la salida llegue a su destinatario. Además, te dice cuáles son las prácticas de gobierno que deberían llevarse a cabo que nos va a dar la entrada. Para cada proceso dentro de cada práctica (actividad) se desarrolla las entradas, salidas y actividades de cada práctica. Así como una guía relacionada de que otras guías te pueden ayudar para cada proceso [7].

## 4.2. ITIL

El segundo marco o framework que vamos a ver es ITIL.

ITIL es una biblioteca (Biblioteca de la Infraestructura de Tecnología de la Información) y está formada por una serie de “Mejores Prácticas” procedentes de todo tipo de suministradores de servicios de TI. [8]

ITIL especifica un método sistemático que garantiza la calidad de los servicios de TI. Ofrece una descripción detallada de los procesos más importantes en una organización de TI, incluyendo listas de verificación para tareas, procedimientos y responsabilidades que pueden servir como base para adaptarse a las necesidades concretas de cada organización.

Al mismo tiempo, el amplio campo de aplicación de ITIL la convierte en una útil guía de referencia en muchas áreas, lo que puede servir a las organizaciones de TI para definir nuevos objetivos de mejora que lleven a su crecimiento y madurez.

ITIL está basado en el concepto de ciclo de vida junto a cuatro fundamentos: las buenas prácticas, la gestión de servicios, los procesos y las funciones. Se centra en el retorno de la experiencia, las buenas prácticas son directrices y tú las adaptas a tu empresa.

Para poder entender ITIL y su ciclo de vida, que explicaré a continuación, voy a definir dos conceptos clave. El primero de ellos es el de servicio: Un servicio es un medio para entregar valor a los clientes, facilitando los resultados que los clientes quieren conseguir sin asumir costes o riesgos específicos. El segundo de los conceptos es gestión de servicios: La Gestión de Servicios es un conjunto de capacidades organizativas especializadas cuyo fin es generar valor para los clientes en forma de servicios.

ITIL está orientado a procesos que son un conjunto estructurado de actividades interrelacionadas que permite alcanzar un objetivo. Hay que definir el proceso, documentarlo y controlarlo. Un proceso utiliza una o varias entradas y las transforma en salidas, así como incluye definición de roles y responsabilidades, es decir, una autoridad asignada a una persona o equipo para un proceso o función, puede tener varios roles. Incluye actividades, procedimientos e instrucciones. Es indispensable que se pueda medir y evaluar un servicio por lo que queremos saber si es eficaz y eficiente. Hay facilitadores del proyecto que son recursos (económicos, software, hardware) y aptitudes (que eres capaz de hacer). Finalmente decir que los procesos son transversales.

Otro concepto clave en ITIL es el de función. Una función es una unidad organizativa con recursos y medios propios, que es responsable de producir un resultado. Una misma función puede llevar a cabo diferentes procesos.

ITIL enfoca la gestión de servicios a partir del Ciclo de Vida de un servicio. El Ciclo de Vida del Servicio es un modelo de organización que ofrece información sobre:

- La forma en que está estructurada la gestión del servicio.
- La forma en que los distintos componentes del Ciclo de Vida están relacionados entre sí.
- El efecto que los cambios en un componente tendrán sobre otros componentes y sobre todo el sistema del Ciclo de Vida.

El Ciclo de Vida del Servicio consta de cinco fases:

1. Estrategia del Servicio: La fase de diseño, desarrollo e implementación de la Gestión del Servicio como un recurso estratégico.
2. Diseño del Servicio: La fase de diseño para el desarrollo de servicios de TI apropiados, incluyendo arquitectura, procesos, política y documentos; el objetivo del diseño es cumplir los requisitos presentes y futuros de la empresa.
3. Transición del Servicio: La fase de desarrollo y mejora de capacidades para el paso a producción de servicios nuevos y modificados.
4. Operación del Servicio: La fase en la que se garantiza la efectividad y eficacia en la provisión y el soporte de servicios con el fin de generar valor para el cliente y el proveedor del servicio.
5. Mejora Continua del Servicio: La fase en la que se genera y mantiene el valor para el cliente mediante la mejora del diseño y la introducción y Operación del Servicio.

La Estrategia del Servicio es el eje en torno al que “giran” todas las demás fases del Ciclo de Vida del Servicio ya que, es la fase de definición de políticas y objetivos. Las fases de Diseño del Servicio, Transición del Servicio y Operación del Servicio ponen en práctica esta estrategia a través de ajustes y cambios. La fase de Mejora Continua del Servicio, que consiste en aprendizaje y mejora, abarca todas las fases del ciclo.



*Ilustración 4. Ciclo de Vida del Servicio*

(Guía de Gestión – ITIL v3)

Fases del ciclo de vida de ITIL v3:

Estrategia de servicio: La Estrategia del Servicio define directrices para el diseño, desarrollo e implantación de la Gestión del Servicio como un recurso estratégico, teniendo en cuenta la estrategia de la empresa.

La Estrategia del Servicio ayuda a las organizaciones a pensar y actuar de una manera estratégica. La estrategia se implementa mediante el uso de activos estratégicos.

Las cuatro actividades más importantes del proceso de Estrategia del Servicio son:

1. Definición del mercado:
  - a. Entendimiento del cliente.
  - b. Entendimiento de las oportunidades.
  - c. Clasificación y visualización de los servicios.
2. Desarrollo de la oferta.
3. Desarrollo de los activos estratégicos.
4. Preparación de la implementación.

Tenemos que identificar y entender las necesidades de los clientes, el mercado, la competencia de la empresa y la competencia de departamento informático.

La estrategia de servicio consta de cinco procesos:

- **Gestión financiera:** Proporciona información vital para que la gestión pueda garantizar una provisión del servicio eficiente y rentable. Una buena Gestión Financiera permite a la organización justificar todos los gastos y asignarlos directamente a servicios.
- **Gestión de la cartera de servicios:** es un método dinámico para gobernar las inversiones en Gestión de Servicios a lo largo de la empresa, y gestionarlas para obtener valor. El objetivo de la Gestión de la Cartera de Servicios es generar el máximo valor controlando riesgos y costes.
- **Gestión de la demanda:** Adapta el suministro a la demanda y tiene como fin predecir con la mayor exactitud la demanda y, si es posible, llegar incluso a regularla. Una demanda mal gestionada supone un riesgo para los proveedores de servicios.
- **Gestión de la estrategia:** Construir la política informática y de sistemas de información para los próximos años. Produce el esquema Director.
- **Gestión de la relación comercial:** Garantizar la satisfacción de las relaciones comerciales con la informática.

Diseño de servicio: El Diseño del Servicio se ocupa del diseño y desarrollo de servicios y sus procesos relacionados. No afecta sólo a los nuevos servicios, sino también a los que han sido modificados. [9]

El objetivo principal del Diseño del Servicio es: El diseño de servicios nuevos o modificados para su paso a un entorno de producción.

Los objetivos del diseño son:

1. Especificar nuevos servicios.
2. Optimizar costes.
3. Identificar y gestionar riesgos.
4. Desarrollar las competencias necesarias para satisfacer las necesidades del cliente.
5. Desarrollar los procesos para satisfacer a los clientes.

Se requiere un enfoque holístico lo que quiere decir que se aborda de manera global, no separando cada una de sus partes sino como un todo.

El diseño de servicios de TI eficaces y eficientes es un proceso que busca el equilibrio de funcionalidad, recursos disponibles (humanos, técnicos y financieros) y tiempo disponible con el fin de satisfacer las necesidades y demandas del negocio.

Las tres actividades del proceso de Diseño de Servicio son:

1. Desarrollo de requisitos
2. Gestión de la información y los datos
3. Gestión de aplicaciones

El diseño de servicio consta de ocho procesos:

- Gestión del Catálogo de Servicios: La meta es el desarrollo y mantenimiento de un Catálogo de Servicios que contenga todos los detalles, el estado, las posibles interacciones y las dependencias mutuas de todos los servicios actuales y de aquellos que estén siendo preparados para su funcionamiento operacional.
- Gestión del Nivel de Servicio: La meta es garantizar que se proporciona un nivel acordado de servicio de TI para todos los servicios de TI actuales, y que los futuros servicios se entreguen de acuerdo a objetivos alcanzables, es decir, gestiona la relación comercial y con los clientes, formalizándola, garantiza respetar los contratos negociados.
- Gestión de la Capacidad: La meta es garantizar que en todas las áreas de TI siempre exista una capacidad de TI justificable en términos de coste, y que ésta se corresponda, de manera oportuna en el tiempo, con las necesidades actuales y futuras acordadas con el negocio.
- Gestión de la Disponibilidad: La meta es garantizar que los niveles de disponibilidad que se entregan en todos los servicios, cumplen o superan las necesidades actuales y futuras acordadas con el negocio, de manera eficiente en costes.
- Gestión de la Continuidad del Servicio de TI: La meta es dar soporte al proceso global de continuidad del negocio, garantizando que todas las instalaciones

técnicas y de servicios de TI necesarias puedan volver a funcionar en los plazos de tiempo requeridos y acordados con el negocio.

- **Gestión de la Seguridad de la Información:** La meta es alinear la seguridad de TI con la del negocio y garantizar una gestión eficaz de la seguridad de la información en todos los servicios y actividades de Gestión del Servicio.
- **Gestión de proveedores:** La meta es gestionar a los proveedores y los servicios que proporcionan, con el fin de conseguir una calidad consistente de los servicios de TI al negocio, garantizando un precio adecuado.
- **Coordinación del diseño:** La meta es coordinar actividades de la fase de diseño de servicios.

Transición del servicio: La Transición del Servicio incluye la gestión y coordinación de los procesos, sistemas y funciones necesarios para la construcción, prueba y despliegue de una “versión” en producción, así como para la definición del servicio según las especificaciones del cliente y las partes interesadas. [10]

Los objetivos de la Transición del Servicio son:

1. Producir los medios necesarios para realizar, planificar y gestionar el nuevo servicio.
2. Minimizar el impacto sobre los servicios que ya están en producción.
3. Aumentar la satisfacción del cliente y fomentar el uso correcto del servicio y la tecnología.

La comunicación es un aspecto fundamental de la Transición del Servicio.

Hay otras actividades importantes en la Transición del Servicio como la gestión de cambios organizativos o la gestión de los grupos de interés.

La transición de servicio consta de siete procesos:

- **Planificación y Soporte de la Transición:** Sus metas son, planificar y coordinar recursos para garantizar el cumplimiento de las especificaciones del Diseño del Servicio e identificar, gestionar y limitar riesgos que puedan interrumpir el servicio a partir de la fase de transición.



- **Gestión de Cambios:** El objetivo es garantizar que todos los cambios se registran, evalúan, autorizan, priorizan, y que su realización, integración y desarrollo siguen procedimientos eficaces y eficientes.
- **Gestión de la Configuración y Activos del Servicio:** El objetivo es definir componentes de servicio e infraestructura y mantener registros de la configuración.
- **Gestión de Entregas y Despliegues:** La meta es poner las entregas en producción y establecer un uso efectivo del servicio, al objeto de entregar valor al cliente y ser capaz de transferir las operaciones del servicio.
- **Validación y Pruebas del Servicio:** Proporciona objetivos esperados para el buen nivel de calidad, garantiza gestión de restricciones, errores y funcionamientos incorrectos, especifica además políticas de validación.
- **Evaluación:** Desencadenado por el proceso de gestión de cambios, determina el rendimiento del cambio y evalúa efectos, impactos y riesgos. Rechaza el cambio antes de entrar en servicio.
- **Gestión del Conocimiento:** El objetivo es proveer información a los informáticos en el momento, tiempo, forma y nivel necesarios y entendible por ellos.

Operación del servicio: Disponer de procesos bien diseñados e implementados sirve de muy poco si no se organiza correctamente la ejecución diaria de dichos procesos. Tampoco es posible introducir mejoras si durante la Operación del Servicio no se realizan sistemáticamente actividades de recopilación de datos y medida del rendimiento diario.

[11]

La Operación del Servicio tiene como objetivos la coordinación y ejecución de las actividades y procesos necesarios para entregar y gestionar servicios para usuarios y clientes con el nivel especificado.

La Operación del Servicio se encarga de realizar todas las actividades necesarias para la prestación y el soporte de servicios. Dichas actividades son las siguientes:

1. Los servicios
2. Los procesos de Gestión del Servicio

3. La tecnología
4. Las personas

La organización del servicio consta de cinco procesos:

- **Gestión de Eventos:** El objetivo de la gestión de eventos es detectar eventos, analizarlos y determinar la acción de gestión apropiada. Proporciona la entrada para la ejecución de un gran número de procesos y actividades de la Operación del Servicio.
- **Gestión de Incidencias:** El objetivo es restaurar el servicio lo más rápido posible para reducir efectos sobre los usuarios.
- **Gestión de Peticiones:** Los objetivos son: poner a disposición de los usuarios un canal a través del cual puedan solicitar y recibir servicios, proporcionar a usuarios y clientes información sobre la disponibilidad de servicios y el procedimiento para obtener dichos servicios, proporcionar los componentes de servicios estándar (licencias y software) y facilitar información general, quejas y comentarios.
- **Gestión de Problemas:** El objetivo es prevenir problemas e incidencias, eliminar la repetición de incidencias y minimizar el impacto de las incidencias que no se puedan evitar.
- **Gestión de Accesos:** El objetivo es gestionar solicitudes relativas a accesos, permisos y privilegios que se asignan a usuarios, gestión de incidencias y grupos.

Mejora continua del servicio: Las organizaciones de TI tienen que alinear y realinear continuamente sus servicios de TI ante las necesidades cambiantes del negocio, identificando e implementando mejoras que sirvan al negocio y para ello está la fase de mejora continua. [12]

La meta es la mejora continua de la eficacia y la eficiencia de servicios de TI para facilitar el cumplimiento de los objetivos de negocio. Esto implica satisfacer y superar los objetivos (eficacia), así como alcanzar dichos objetivos con el menor coste posible (eficiencia).

Los principales objetivos son:

1. Medir y analizar logros de nivel de servicio comparándolos con los requisitos estipulados en el acuerdo de nivel de servicio.
2. Recomendar mejoras en todas las fases del Ciclo de Vida.
3. Introducir actividades que aumenten la calidad, la eficiencia, la eficacia y la satisfacción del cliente en los servicios y en los procesos de la Gestión de Servicios de TI.
4. Operar servicios de TI más rentables sin que se resienta la satisfacción del cliente.
5. Utilizar métodos de Gestión de Calidad adecuados para actividades de mejora.

Hay métricas para comparar los resultados con los niveles deseados y hay 7 etapas para gestionar el despliegue de los puntos de mejora.

Finalmente comentaré las funciones de ITIL de manera muy resumida.

#### Funciones de ITIL:

- Centro de servicios: Gestiona toda la relación con las personas que utilizan la informática.
- Gestión de operaciones: Garantizar estabilidad y disponibilidad de los sistemas.
- Gestión técnica: Definir, planificar, implementar y mantener una infraestructura técnica estable.
- Gestión de aplicaciones: Proporcionar experiencia para soportar los procesos de negocio.

### 4.3. ISO 38500

El último de los frameworks que vamos a ver es la ISO 38500.

La ISO 38500 es un sistema para la normalización a nivel mundial y que colabora en campos de interés mutuo, donde el ISO/IEC JTC 1 es el comité técnico para el campo de tecnologías de la información y la ISO/IEC 38500 originalmente fue la AS 8015:2005 que emana de otro anterior llamado el informe Cadbury. [13]

La ISO 38500 es un estándar que son normas de alto nivel, es decir indican lo que hay que hacer, pero no como llevarlo a cabo, cuyo objetivo es ser un marco de principios para los administradores para evaluar, dirigir y supervisar el uso de TI en la organización. Es un marco para la gobernanza TI que ayuda a las organizaciones a entender y cumplir con obligaciones legales, reglamentos y ética.

El objeto de la ISO 38500 es proporcionar principios orientadores a la parte alta de la empresa como altos directivos, miembros de grupos de monitorización, especialistas externos, entre otros. Si se siguen los principios se está intentando asegurar que tu empresa es eficaz, eficiente y aceptable ya que se aplica sobre gobernanza de procesos y decisiones de gestión relativos a la TI.

El campo de aplicación es en todas las organizaciones ya sean públicas, privadas, grandes, pequeñas, etc. y con el objetivo de que sean eficaces, eficientes y aceptables en TI ya que al llevar a cabo esta norma lo que logras es que se pueda confiar en que la parte de gobierno está haciendo un buen uso de TI, además de informar y orientar a los administradores y de implantar organismos de medición objetiva.

La gobernanza corporativa TI ayuda, entre otras cosas a, la adecuada implementación y explotación de los activos TI, a la continuidad y sostenibilidad del negocio, a la alineación TI con negocio, a la reducción de costes, en definitiva, la idea es exprimir al máximo que se pueda la TI para aprovechar al máximo la inversión.

La norma tiene principios y un modelo basado en actividades. Hay seis principios que son los comportamientos deseables para la toma de decisión. Y tres modelos que son los que van a dar orientación para asegurar que van a cumplirse los principios.

Los principios son:

1. Responsabilidad: entender, asumir y aceptar sus responsabilidades; la persona que tiene la responsabilidad tiene que tener la capacidad para llevar esas acciones a cabo.
2. Estrategia: la estrategia de negocio de la organización tiene en cuenta las capacidades actuales y futuras de la TI; los planes de la TI satisfacen las necesidades actuales y futuras de la estrategia de negocio.

3. Adquisición: vamos a adquirir tecnología por lo que tenemos que asegurarnos que vamos a comprarla de manera adecuada, es decir, la adquisición debe ser equilibrada entre lo que gastas y lo que necesitas o amortizas.
4. Desempeño: la tecnología se utiliza para proveer los servicios necesarios para la empresa, por lo que hay que mirar que de verdad sirve a los propósitos, es decir, tiene que dar soporte a la misión de la empresa.
5. Cumplimiento: la TI cumple con toda la legislación y normativas obligatorias. Las políticas están claramente definidas, implantadas y se hacen cumplir.
6. Conducta humana: significa que las personas están utilizando la TI para lo que es.

Las actividades que componen el modelo:

- Evaluar el uso actual y futuro de la TI: valorar la situación y emitir juicios, como también considerar presiones externas. Hay que tener en cuenta las necesidades que tu negocio va a tener en función de los objetivos. Y debe hacerse de forma continua.
- Dirigir la preparación y ejecución de planes y políticas para asegurar que el uso de la TI satisface los objetivos de la organización: implica asignación de responsabilidades y prepara la empresa para implantar esos planes de acción dando los recursos necesarios o lo que es lo mismo trazar las acciones necesarias y establecerlas para llevar un buen gobierno TI.
- Monitorizar el cumplimiento de las políticas y el desempeño con relación a lo planificado: tiene que ver que esas acciones que se están llevando a cabo están dando su fruto. Hay que medir, establecer métricas e índices de esas métricas.

## 4.4. Conclusión

Como conclusión de este apartado del estado del arte decir que, aunque los tres marcos comentados anteriormente tienen similitudes, COBIT y la ISO 38500 indican el “Qué”, mientras que ITIL indica el “Cómo” por lo que COBIT y la ISO 38500 son normas de alto nivel que van a ser más generales y que seguro que vamos a poder aplicar para mejorar

la asociación que estamos auditando, aunque como ITIL tiene tantos procesos, seguro que la implantación de algunos de ellos va a ser útiles para la asociación, por lo que de momento no podemos decir que un marco es mejor que otro sin auditar.

Lo más posible es que no apliquemos un marco entero, pero de los tres que he comentado anteriormente voy a extraer, después de auditar, tareas, procesos o principios que nos van a servir para mejorar el estado de la empresa.

## 5.- Estado del arte: Auditorías y como realizarlas

En este apartado vamos a recoger los principales aspectos referentes a la auditoría informática, ya que, como hemos comentado en el análisis DAFO, desconocemos como se realizan y hemos tenido que buscar mucha información sobre los pasos que se deben realizar y como debe ser desde diferentes puntos de vista, por lo que antes de decidir una manera de realizarla vamos a recoger y estructurar las principales propuestas que hemos pensado que nos resultaría útil de cara a realizar la auditoría.

La auditoría es una actividad que, aunque tiene una finalidad global clara que es, evaluar las TI dentro de una organización respecto a los procesos, servicios, aplicaciones, infraestructura e información, identificando riesgos de negocio relacionados con TI, su metodología es diversa y dependiendo de los autores los procesos y enfoques pueden cambiar, aunque al final se tratan de distintas formas de abordar un mismo problema. Es por ello que primero, y en un escenario de desconocimiento por falta de experiencia, es mejor comenzar explorando las propuestas actuales para después decantarnos por aquella o la combinación de aquellas que creamos que mejor nos va a resultar.

Para poder realizar una auditoría necesitamos obtener información acerca de los pasos que tenemos que seguir para realizarla y que tenemos que realizar en cada paso, así como herramientas o técnicas para realizar una auditoría como pueden ser cuestionarios, entrevistas, checklist o trazas y/o huellas. Después de buscar mucha información en diversas fuentes, hemos considerado oportuno comentar distintas guías o metodologías que describen el proceso a seguir, donde hemos podido observar similitudes, pero también diferencias, así como un cuestionario que, con un pequeño esfuerzo para adecuarlo a la Asociación APSA, nos podría resultar de gran utilidad.

## 5.1. Guía para realizar una auditoría informática paso a paso

Esta guía indica los pasos que hay que seguir para realizar una auditoría informática que son, análisis, planificación, determinación de riesgos e incidencias y ejecución, así como una breve explicación de que se debe hacer en cada uno de ellos. [14]

El primer paso es el análisis y la información sobre este paso es: No todas las empresas tienen los mismos objetivos cuando encargan una auditoría informática. Quizás, su red informática es perfecta y sus equipos físicamente no les producen el menor problema. Pero sí tienen problemas en cuanto a la seguridad informática de los equipos. Por tanto, el primer paso en una auditoría será determinar los objetivos que se tienen y, en segundo lugar, hacer un inventario de todos los aspectos concernientes a los sistemas y usos informáticos en la empresa, con lo que será inevitable una estrecha colaboración entre gerente, empleados y técnicos informáticos.

El segundo paso es la planificación y su información es la siguiente: Cuando tenemos claros los objetivos de la auditoría informática y tenemos un inventario de los componentes informáticos que hay, así como los usos más habituales dentro de la empresa, planificamos nuestra auditoría a través de herramientas de análisis. Cómo vamos a evaluar cada uno de los puntos que hemos analizado y de acuerdo con qué criterios. Por ejemplo, puede que el empresario quiera saber si sus equipos informáticos son los más idóneos para ofrecer un servicio efectivo en producción de vídeos. El resultado de la auditoría puede ser, por ejemplo, que para cumplir sus objetivos el material del que dispone no es lo suficiente efectivo.

El tercer paso es determinación e incidencias y su información es: El mantenimiento preventivo y predictivo es clave en toda auditoría informática. No se trata sólo de analizar ahora cuántas incidencias o problemas se están produciendo en este momento, sino los posibles riesgos que existen de que se produzca un problema en el futuro. Las empresas deben prever estos problemas mediante unas prácticas de mantenimiento efectivas, sobre todo en cuanto a seguridad informática.



El cuarto y último paso es la ejecución de la auditoría y la información relativa a este es: Por último, se tomarán medidas ejecutivas para resolver los problemas que ya están produciendo y prevenir los riesgos que se podrían producir. A partir de ahí, lo normal es elaborar un presupuesto con los puntos que habría que corregir para que se cumplan los objetivos de la empresa, ya sea mejorar la seguridad informática porque han tenido problemas de ataques informáticos, o adecuar sus sistemas a un determinado objetivo de productividad.

Esta guía constituye una metodología simple y clara, aunque demasiado abstracta, de los pasos que se deben realizar en una auditoría, por lo que nos sirve para tener claros cuáles serán los pasos a seguir, pero no nos aporta mucha información más.

## 5.2. Auditoría Informática Planificación

En [15] podemos encontrar otra propuesta que explica brevemente lo que hay que hacer para realizar una auditoría informática de manera más desglosada que en el punto anterior ya que se divide en los siguientes puntos: alcance y objetivos, estudio inicial, entorno operacional, determinación de recursos de la Auditoría informática, perfiles de los auditores, elaboración del plan y de los programas de trabajo, objetivos a evaluar, un resumen.

Los pasos a seguir son:

1. Alcance y objetivos y este punto dice que, las personas que realizan la auditoría han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar. Deben comprender los deseos y pretensiones del cliente, de forma que las metas fijadas puedan ser cumplidas.
2. Estudio inicial y en él se explica que, para realizar dicho estudio ha de examinarse las funciones y actividades generales de la informática.

Para su realización el auditor debe conocer lo siguiente:

1. Organigrama
2. Departamentos

3. Número de puestos de trabajo
4. Número de personal por puestos de trabajo

3. Entorno operacional y dice que, el equipo de auditoría informática debe poseer una adecuada referencia del entorno en el que va a desenvolverse.

- 1) Situación geográfica de los sistemas
- 2) Arquitectura y configuración de Hardware y Software
- 3) Inventario de Hardware y Software
- 4) Comunicación y redes de comunicación

Igualmente, poseerán información de las redes locales de la empresa, aplicaciones bases de datos y ficheros, etc.

4. Determinación de recursos de la Auditoría Informática y se explica que, mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

5. Perfiles de los auditores y, en la tabla que hay a continuación se van a explicar que perfiles deberían tener los auditores y los conocimientos que deberían tener, así como las actividades que van a deberían desempeñar en la auditoría.

*Tabla 4. Perfiles de los auditores*

<b>Profesión</b>	<b>Actividades y conocimientos deseables</b>
Informático en general	Con experiencia amplia en ramas distintas. Es deseable que su labor se haya desarrollado en explotación y en desarrollo de proyectos. Conocedor de sistemas.
Experto en desarrollo de proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de desarrollo más importantes.
Técnico de Sistemas	Experto en sistemas operativos y software básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de explotación.
Experto en bases de datos y administración de las mismas	Con experiencia en el mantenimiento de bases de datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación.
Experto en software de comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en subsistemas de telescopio.

Experto en explotación y gestión de CPD'S	Responsable de algún centro de cómputos. Amplia experiencia en automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.
Técnico de organización	Experto organizador y coordinador. Especialista en el análisis de flujo de información.
Técnico de evaluación de costes	Economista con conocimiento de Informática. Gestión de costes

6. Elaboración del plan y de los programas de trabajo y este punto dice que, en la etapa de planeación de la auditoría deben intervenir todas las áreas de la organización que permitirán llevar a cabo la realización del proyecto

7. Objetivos a evaluar y son los siguientes:

- Evaluación de los sistemas y procedimientos
- Evaluación de los equipos de cómputo
- Evaluación del proceso de datos

Y dentro de la planificación se deben incluir y documentar los siguientes puntos:

- Definir los objetivos y alcance del trabajo
- Los recursos que se necesitaran para la auditoría
- Canales de comunicación entre los involucrados del proyecto
- Inspección detallada de las actividades a auditar
- Asignar responsables de revisar los resultados de la auditoría

En resumen, de la planificación dependerá la eficiencia y efectividad del logro de los objetivos propuestos utilizando los recursos estrictamente necesarios.

La planificación debe ser cuidadosa y seleccionar los métodos más apropiados para realizar las tareas, por lo tanto, los responsables de la planificación deben ser los miembros más experimentados del equipo.

## 5.3. Metodología para realizar una auditoría

En [16] podemos encontrar otra propuesta que explica, como en los anteriores, los pasos o etapas que debe seguir una auditoría, pero con diferencias con respecto a los anteriores, ya que esta metodología se divide en etapa de planeación de la auditoría, etapa de ejecución de la auditoría y etapa de dictamen de la auditoría. En cada una de estas etapas, se explica que hay dentro de ellas y se dividen en sub apartados para desglosar más cada etapa y que así se puede realizar de una mejor forma.

### 5.3.1. Etapa de Planeación de la Auditoría

La primera etapa es la Etapa de Planeación de la Auditoria y en ella se explica lo siguiente: El primer paso para realizar una auditoría de sistemas es la planeación de cómo se va a ejecutar la auditoria, donde se debe identificar de forma clara las razones por las que se va a realizar la auditoria, la determinación del objetivo de la misma, el diseño de métodos, técnicas y procedimientos necesarios para llevarla a cabo y para la solicitud de documentos que servirán de apoyo para la ejecución, terminando con la elaboración de la documentación de los planes, programas y presupuestos para llevarla a cabo.

Para ello hay que seguir una serie de pasos:

1. Identificar el origen de la auditoria: Este es el primer paso para iniciar la planeación de la auditoria, en esta se debe determinar por qué surge la necesidad o inquietud de realizar una auditoría. Las preguntas que se deben contestar ¿de dónde?, ¿por qué?, ¿quién? o ¿para qué? Se quiere hacer la evaluación de algún aspecto de los sistemas de la empresa.

2. Visita Preliminar al Área informática: Este es el segundo paso en la planeación de la auditoria y consiste en realizar una visita preliminar al área de informática que será auditada, luego de conocer el origen de la petición de realizar la auditoria y antes de iniciarla formalmente; el propósito es el de tener un primer contacto con el personal asignado a dicha área, conocer la distribución de los sistemas y donde se localizan los servidores y equipos terminales en el centro de cómputo, sus características, las

medidas de seguridad y otros aspectos sobre que problemáticas que se presentan en el área auditada.

Aquí se deben tener en cuenta aspectos tales como:

- La visita inicial para el arranque de la auditoria cuya finalidad es saber ¿Cómo se encuentran distribuidos los equipos en el área?, ¿Cuántos, cuáles, cómo y de que tipo son los servidores y terminales que existen en el área?, ¿Qué características generales de los sistemas que serán auditados?, ¿Qué tipo de instalaciones y conexiones físicas existen en el área?, ¿Cuál es la reacción del personal frente al auditor?, ¿Cuáles son las medidas de seguridad física existentes en el área?, y ¿Qué limitaciones se observan para realizar la auditoria?. Con esta información el auditor podrá diseñar las medidas necesarias para una adecuada planeación de la auditoria y establecer algunas acciones concretas que le ayuden al desarrollo de la evaluación.

3. Establecer los Objetivos de la Auditoria: Los objetivos de la planeación de la auditoria son:

- *El objetivo general* que es el fin global de lo que se pretende alcanzar con el desarrollo de la auditoría informática y de sistemas, en él se plantean todos los aspectos que se pretende evaluar.

- *Los objetivos específicos* que son los fines individuales que se pretenden para el logro del objetivo general, donde se señala específicamente los sistemas, componentes o elementos concretos que deben ser evaluados.

4. Determinar los Puntos que serán evaluados: Una vez determinados los objetivos de la auditoria se debe relacionar los aspectos que serán evaluados, y para esto se debe considerar aspectos específicos del área informática y de los sistemas computacionales tales como: la gestión administrativa del área informática y el centro de cómputo, el cumplimiento de las funciones del personal informático y usuarios de los sistemas, los sistemas en desarrollo, la operación de los sistemas en producción, los programas de capacitación para el personal del área y usuarios de los sistemas, protección de las bases

de datos, datos confidenciales y accesos a las mismas, protección de las copias de seguridad y la restauración de la información, entre otros aspectos.

5. Elaborar Planes, programas y Presupuestos para Realizar la auditoria: Para realizar la planeación formal de la auditoria informática y de sistemas, en la cual se concretan los planes, programas y presupuestos para llevarla a cabo se debe elaborar los documentos formales para el desarrollo de la auditoria, donde se delimiten las etapas, eventos y actividades y los tiempos de ejecución para el cumplimiento del objetivo, anexando el presupuesto con los costos de los recursos que se utilizarán para llevarla a cabo.

Algunos de los aspectos a tener en cuenta serán: Las actividades que se van a realizar, los responsables de realizarlas, los recursos materiales y los tiempos; el flujo de eventos que sirven de guía; la estimación de los recursos humanos, materiales e informáticos que serán utilizados; los tiempos estimados para las actividades y para la auditoria; los auditores responsables y participantes de las actividades; otras especificaciones del programa de auditoría.

6. Identificar y seleccionar los Métodos, herramientas, Instrumentos y Procedimientos necesarios para la Auditoria: En este se determina la documentación y medios necesarios para llevar a cabo la revisión y evaluación en la empresa, seleccionando o diseñando los métodos, procedimientos, herramientas, e instrumentos necesarios de acuerdo a los planes, presupuestos y programas establecidos anteriormente para la auditoria. Para ello se debe considerar los siguientes puntos: establecer la guía de ponderación de cada uno de los puntos que se debe evaluar; elaborar una guía de la auditoria; elaborar el documento formal de la guía de auditoría; determinar las herramientas, métodos y procedimientos para la auditoria de sistemas; diseñar los sistemas, programas y métodos de pruebas para la auditoria.

7. Asignar los Recursos y Sistemas computacionales para la auditoria: Finalmente se debe asignar los recursos que serán utilizados para realizar la auditoria. Con la asignación de estos recursos humanos, informáticos, tecnológicos y de cualquier otro tipo se llevará a cabo la auditoria.

### 5.3.2. Etapa de Ejecución de la Auditoría

La segunda etapa es la Etapa de Ejecución de la Auditoría y es la ejecución de la misma, y está determinada por las características propias, los puntos elegidos y los requerimientos estimados en la planeación.

### 5.3.3. Etapa de Dictamen de la Auditoría

La tercera etapa después de la planeación y ejecución es la Etapa de Dictamen de la Auditoría que es el resultado final de la auditoría, donde se presentan los siguientes puntos: la elaboración del informe de las situaciones que se han detectado, la elaboración del dictamen final y la presentación del informe de auditoría de la siguiente manera:

1. Analizar la información y elaborar un informe de las situaciones detectadas: Junto con la detección de las oportunidades de mejoramiento se debe realizar el análisis de los papeles de trabajo y la elaboración del borrador de las oportunidades detectadas, para ser discutidas con los auditados, después se hacen las modificaciones necesarias y posteriormente el informe final de las situaciones detectadas.

2. Elaborar el Dictamen Final: El auditor debe terminar la elaboración del informe final de auditoría y complementarlo con el dictamen final, para después presentarlo a los directivos del área auditada para que conozcan la situación actual del área, antes de presentarlo al representante o gerente de la empresa.

Una vez comentadas las desviaciones con los auditados, se elabora el informe final, lo cual es garantía de que los auditados ya aceptaron las desviaciones encontradas y que luego se llevan a documentos formales.

3. Elaborar el Dictamen Formal: El último paso de esta metodología es presentar formalmente el informe y el dictamen de la auditoría al más alto de los directivos de la empresa donde se informa de los resultados de la auditoría. Tanto el informe como el dictamen deben presentarse en forma resumida, correcta y profesional. La presentación de la misma se hace en una reunión directiva y por eso es indispensable usar un lenguaje claro tanto en el informe como en la exposición del mismo. El informe debe contener

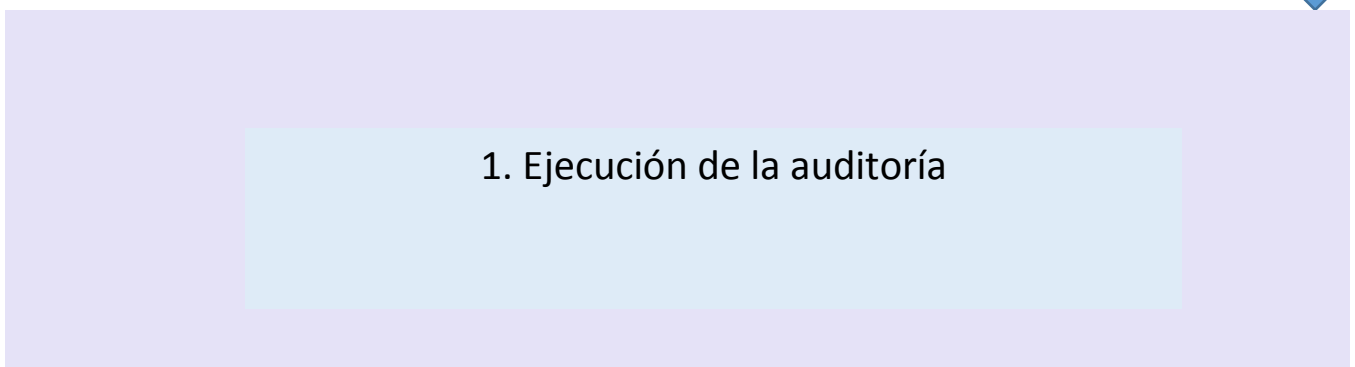
los siguientes puntos: la carta de presentación, el dictamen de la auditoría, el informe de situaciones relevantes y los anexos y cuadros estadísticos.

Al elaborar el dictamen formal se hace tomando en cuenta el informe comentado a los directivos, junto al informe de hallazgos o desviaciones y los papeles de trabajo de cada uno de los auditores. La integración del dictamen y el informe final de auditoría deben ser elaborados con la máxima perfección, tratando de evitar errores. También deben contener de manera clara y concreta, las desviaciones detectadas en la evaluación.

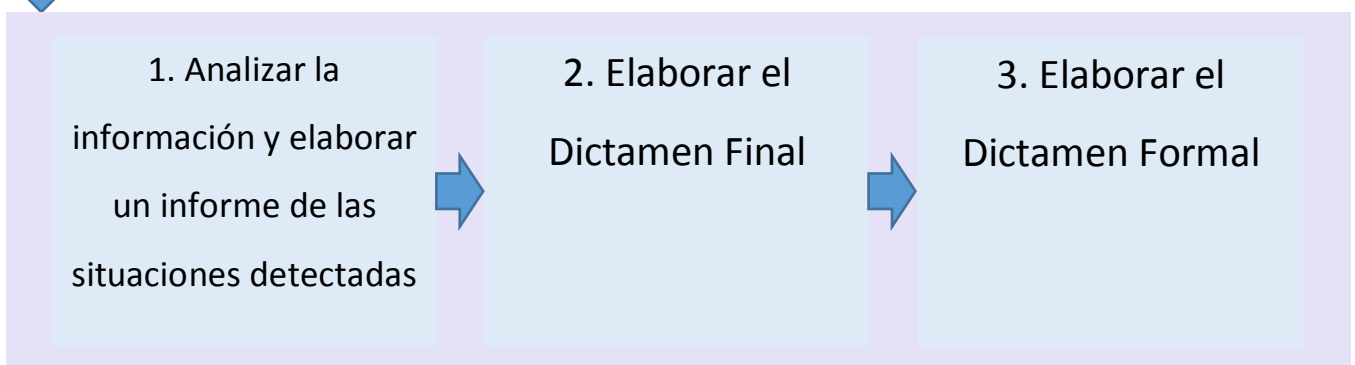
#### Etapa de Planeación de la Auditoría



#### Etapa de Ejecución de la Auditoría



#### Etapa de Dictamen de la Auditoría





Como podemos observar en la ilustración anterior, podemos encontrar un parecido con ITIL ya que, ITIL son procesos que se dividen en actividades y esta metodología son etapas que se dividen en actividades.

## 5.4. Pasos para realizar una auditoría en sistemas informáticos

En [17] podemos encontrar otra propuesta que explica, como en los puntos anteriores, los pasos que debe seguir una auditoría informática con una visión diferente y que como las anteriores, nos va a servir para obtener información sobre los pasos que debemos seguir al realizar la auditoría. En este caso, los pasos van a ser planeación (desde dos puntos de vista: evaluación de los sistemas y procedimientos y evaluación de los equipos de cómputo), alcances y objetivos y estudio inicial de la organización, un informe final, el entorno operacional, aplicaciones de bases de datos y ficheros, actividades de la auditoría informática, determinación de recursos de la auditoría informática, un cuerpo expositivo y finalmente, elaboración del plan y de los programas de trabajo, como se muestra a continuación.

Para hacer una adecuada planeación de la auditoría en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de áreas dentro del organismo a auditar, sus sistemas, organización y equipo.

- En el caso de la auditoría en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de los dos objetivos:
  1. Evaluación de los sistemas y procedimientos: Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar.
  2. Evaluación de los equipos de cómputo: Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base a esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal

necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

- Alcances y objetivos: El alcance de la auditoría expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones a auditar.
- Estudio inicial: Para realizar dicho estudio han de examinarse las funciones y actividades generales de la informática. Para su realización el auditor debe conocer lo siguiente:

#### 1) Organización

- Organigrama: El organigrama expresa la estructura oficial de la organización a auditar. Si se descubriera que existe un organigrama fático diferente al oficial, se pondrá de manifiesto tal circunstancia.
- Departamentos: Se entiende como departamento a los órganos que siguen inmediatamente a la Dirección.
- Relaciones jerárquicas y funciones entre órganos de la Organización: El equipo auditor verificará si se cumplen las relaciones funcionales y jerárquicas previstas por el organigrama, o por el contrario detectará, por ejemplo, si algún empleado tiene dos jefes.
- Flujos de Información: Además de las corrientes verticales intradepartamentales, la estructura organizativa cualquiera que sea, produce corrientes de información horizontales y oblicuas extradepartamentales.
- Número de puestos de trabajo: El equipo auditor comprobará que los nombres de los puestos de trabajo de la organización corresponden a las funciones reales distintas.
- Número de personas por puesto de trabajo: Es un parámetro que los auditores informáticos deben considerar. La inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

- #### 2) Informe final: El informe comienza con la fecha de comienzo de la auditoria y la fecha de redacción del mismo. Se incluyen los nombres del equipo

auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente.

3) Entorno operacional

- Situación geográfica de los sistemas: Se determinará la ubicación geográfica de los distintos centros de proceso de datos en la empresa. A continuación, se verificará la existencia de responsables en cada uno de ellos, así como el uso de los mismos estándares de trabajo.
- Arquitectura y configuración de hardware y software: Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado.
- Inventario de hardware y software: El auditor recabará información escrita, de donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a hardware figurarán las CPUs, unidades de control local y remotas, periféricos de todo tipo, etc.

4) Aplicaciones bases de datos y ficheros: El estudio inicial que han de realizar los auditores se cierra y culmina con una idea general de los procesos informáticos realizados en la empresa auditada. Para ello deberán conocer lo siguiente:

- Volumen, antigüedad y complejidad de las aplicaciones metodología del diseño.
- El auditor recabará información de tamaño y características de las bases de datos, clasificándolas en relación y jerarquías.

5) Actividades de la auditoría informática: La auditoría informática general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos.

6) Determinación de recursos de la auditoría informática: Mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

7) Cuerpo expositivo

- a) Situación actual. Se expondrá la situación prevista y la situación real del lugar.
  - b) Tendencias. Se tratarán de hallar parámetros que permitan establecer tendencias futuras.
  - c) Puntos débiles y amenazas
  - d) Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.
  - e) Redacción posterior de la carta de introducción o presentación
- 8) Elaboración del plan y de los programas de trabajo: Una vez asignados los recursos, el responsable de la auditoría y sus colaboradores establecen un plan del trabajo. Decidido éste, se procede a la programación del mismo.

## 5.5. Procedimientos para la captura de información en la auditoría informática

Una de las partes más importantes en una auditoría es la captura de información y, como ya hemos comentado en la introducción de este apartado, esta captura se suele realizar a través de cuestionarios, entrevistas, checklists o trazas y/o huellas, por lo que después de analizar varias propuestas y opciones, vamos a decantarnos por revisar una propuesta que metodiza dicho proceso.

En [18] se sistematiza la obtención de información para la auditoría, dividiendo el dicho proceso en varios apartados. El primer apartado es el correspondiente al área de planificación. El segundo apartado es el correspondiente al desarrollo de proyectos. El tercer apartado es el correspondiente a los dispositivos de almacenamiento. El cuarto el correspondiente al mantenimiento. El quinto es el de funcionamiento del centro de cómputo. Y finalmente está el de seguridad física.

El apartado correspondiente a la planificación se divide en las preguntas correspondientes a sistemas de información, a recursos humanos y a otros aspectos correspondientes al área de planificación, teniendo como objetivo sondear la

planeación que se realizó para formar el área de sistemas, siendo de vital importancia para el desempeño del área, pues verifica si los objetivos y los alcances del área corresponden a los desempeñados. Algunas de las preguntas que podemos encontrar son:

¿La dirección general y ejecutiva ha considerado la importancia que tiene el estudio del sistema de información?

¿Los informáticos reciben noticias del momento tecnológico por revistas, notas técnicas, etc.?

¿La entidad dispone de un plan informático?

El apartado correspondiente al desarrollo de proyectos tiene como objetivo sondear la elaboración de un proyecto informático, así sea el desarrollo de una aplicación, el mantenimiento de una red de computadoras o para la mayoría de las actividades que se realizan en el área de sistemas. Podemos encontrar preguntas relacionadas con la gestión de proyectos, como puede ser:

¿Existe una lista de proyectos de sistema de procedimiento de información y fechas programadas de implantación que puedan ser considerados como plan maestro?

¿Quién interviene en la planeación de los proyectos?

El apartado correspondiente a los dispositivos de almacenamiento tiene como objetivo evaluar la administración, la aplicación y el uso de dispositivos, hardware, de almacenamiento de información electrónico de la organización. Podemos encontrar preguntas como:

Los locales asignados a los servidores de datos tienen

- Aire acondicionado ( )

- Protección contra el fuego ( )
- (Señalar que tipo de protección) \_\_\_\_\_
- Cerradura especial ( )
- Otra

¿Se certifica la destrucción o baja de los archivos defectuosos?

SI ( ) NO ( )

El apartado correspondiente al mantenimiento tiene como objetivo evaluar las tareas correspondientes al mantenimiento del activo informático y tiene preguntas del estilo de:

¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo?

SI ( ) NO ( )

¿Existen tiempos de respuesta y de compostura estipulados en los contratos?

SI ( ) NO ( )

El apartado correspondiente al funcionamiento del centro de cómputo tiene como objetivo evaluar el correcto funcionamiento, así como la organización del centro de cómputo, tomando en cuenta los reglamentos del área. Así como también revisar que estos reglamentos tengan como objetivo mantener el orden del centro de cómputo. Teniendo preguntas como:

¿Se tiene asignado un lugar específico para papelería y utensilios de trabajo?

SI ( ) NO ( )

¿Existen prohibiciones para fumar, tomar alimentos y refrescos en el departamento de cómputo?

SI ( ) NO ( )

El apartado correspondiente a la seguridad física verifica la seguridad física de las instalaciones que utiliza el área de sistemas, ya que de esto depende la continuidad de los servicios que presta el área a la organización, en cuanto a necesidades de información. Teniendo preguntas como:

¿Se tienen establecidos procedimientos de actualización a estas copias?

SI ( ) NO ( )

¿Se ha establecido que información puede ser accedida y por qué persona?

SI ( ) NO ( )

Para acceder a este documento completo véase la referencia [19] donde podemos encontrar el cuestionario completo donde se detallan las preguntas que componen los cuatro apartados y que nos permiten tener una vista objetiva del estado, composición, procedimientos, problemáticas y actores de TI en la empresa.

## 5.6. Auditoría de Tecnologías y Sistemas de Información

Aunque en los anteriores apartados ya hemos hablado de los puntos que hay que seguir para realizar una auditoría, así como también de un cuestionario para realizar una revisión informática, en [19] podemos encontrar una explicación más extensa sobre la auditoría de tecnologías y sistemas de información, pero solo vamos a comentar las cosas que más nos han llamado la atención de cara a realizar la auditoría. Vamos a dividir este apartado en los puntos: auditoría informática, el plan auditor informático, el contrato de auditoría y principales áreas de la auditoría informática.

### 5.6.1 Auditoría Informática

El primer punto, llamado Auditoría Informática se expone una breve explicación de lo que es la auditoría informática, cuáles son sus objetivos y cuáles son las funciones de un auditor:

La Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. De este modo la auditoría informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoría:

- Objetivos de protección de activos e integridad de datos.
- Objetivos de gestión que abarcan, no solamente los de protección de activos, sino también los de eficacia y eficiencia.

El auditor evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informativos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso del software. En muchos casos, ya no es posible verificar manualmente los procedimientos informatizados que resumen, calculan y clasifican datos, por lo que se deberá emplear software de auditoría y otras técnicas por ordenador.

El auditor es responsable de revisar e informar a la Dirección de la Organización sobre el diseño y el funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada.

Se pueden establecer tres grupos de funciones a realizar por un auditor informático:

- Participar en las revisiones durante y después del diseño, realización, implantación y explotación de aplicaciones informativas, así como en las fases análogas de realización de cambios importantes.
- Revisar y juzgar los controles implantados en los sistemas informativos para verificar su adecuación a las órdenes e instrucciones de la Dirección, requisitos legales, protección de confidencialidad y cobertura ante errores y fraudes.
- Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información.



### 5.6.2 El Plan Auditor Informático

El segundo punto, que es el Plan Auditor Informático y este es el esquema metodológico más importante del auditor informático. En este documento se debe describir todo sobre esta función y el trabajo que realiza en la entidad.

Las partes de un plan auditor informático deben ser al menos las siguientes:

- Funciones. Ubicación de la figura en el organigrama de la empresa. Debe existir una clara segregación de funciones con la Informática y de control interno informático y este debe ser auditado así mismo. Deben describirse las funciones de forma precisa, y la organización interna del departamento, con todos sus recursos.
- Procedimientos para las distintas tareas de las auditorías.
- Tipos de auditorías que realiza. Metodologías y cuestionarios de las mismas.
- Sistema de evaluación y los distintos aspectos que evalúa. Independientemente de que exista un plan de acciones en el informe final, debe hacerse el esfuerzo de definir varios aspectos a evaluar.
- Nivel de exposición.
- Seguimiento de las acciones correctoras.
- Plan quinquenal. Todas las áreas a auditar deben corresponderse con cuestionarios metodológicos y deben repartirse en cuatro o cinco años de trabajo. Esta planificación además de las repeticiones y añadido de las auditorías no programadas que se estimen oportunas deberán componer anualmente el plan de trabajo anual.
- Plan de trabajo anual. Deben estimarse tiempos de manera racional y componer un calendario que una vez terminado me dará un resultado de horas de trabajo previstas y por tanto los recursos que se necesitarán.
- Debemos hacer notar que es interesante tener una herramienta programada con metodología abierta que permita confeccionar los cuestionarios de las distintas auditorías y fácilmente cubrir los hitos y fases de los programas de trabajo una vez definida la metodología completa.

### 5.6.3. Contrato de Auditoría

En el tercer punto voy a hablar de una pequeña introducción al Contrato de Auditoría y este contrato describe las fases en que se puede descomponer un proceso de decisión en auditoría y una propuesta de esquema podría ser la siguiente:

1. Orientación: el auditor obtiene conocimientos sobre las operaciones del cliente y su entorno y hace una valoración preliminar del riesgo y de la importancia relativa.
2. Evaluación preliminar de los controles internos.
3. Planificación táctica de la auditoría.
4. Elección de un plan para la auditoría.
5. Prueba de cumplimiento de los controles.
6. Evaluación de los controles internos basada en los resultados de las pruebas de cumplimiento.
7. Revisión del plan de auditoría preliminar.
8. Elección de un plan revisado para la auditoría.
9. Realización de pruebas sustantivas.
10. Evaluación y agregación de los resultados.
11. Evaluación de la evidencia. Podría dar lugar a unas pruebas más exhaustivas o formar la base de la elección de la opinión por el auditor.
12. Elección de una opinión que clasifique los estados financieros del cliente.
13. Informe de auditoría.

### 5.6.4 Principales áreas de la auditoría informática

Finalmente, voy a comentar cuáles son las Principales áreas de la auditoría informática que se describen en [19]. Las áreas que se deberían analizar en una auditoría según el libro que se menciona en [19], son las siguientes:

- Auditoría de Outsourcing
- Auditoría de la Seguridad Física
- Auditoría de la Dirección
- Auditoría de Explotación

- Auditoría de Bases de Datos
- Auditoría de Técnicas de Sistemas
- Auditoría de la seguridad
- Auditoría de Redes
- Auditoría de Desarrollo
- Auditoría de Aplicaciones
- Auditoría de Internet
- Auditoría de la Videovigilancia
- Auditoría reglamentaria de los datos de carácter personal

## 5.7. Conclusiones

La conclusión que hemos podido sacar después de realizar este apartado del estado del arte correspondiente a la auditoría es que, como mínimo, una auditoría va a tener las siguientes etapas: primero, un análisis para ver qué objetivos tiene la empresa o en nuestro caso, asociación; después una planificación para ver lo que se va a realizar; tercero, se va a tener que realizar la auditoría, pudiendo utilizar para ello un cuestionario como el que se ha mencionado en el apartado correspondiente; y cuarto presentar unos resultados de la auditoría donde se va a poder observar que deficiencias o fallos tiene la asociación para poder mejorarla con buenas prácticas u otras soluciones.

## 6.- Estado del arte: Inventario

En la primera reunión con los de la Asociación APSA, nos comentaron que no tenían ningún software para el inventario y que utilizaban el Excel para ello. Por lo que, sabiendo que es una de las cosas que se van a mejorar después de realizar la auditoría, puesto que ya hemos visto que es uno de los errores y las posibles mejoras, vamos a poner en esta parte algunos programas, casi todos de código abierto, que van a servir para realizar el inventario.

El inventario es una relación detallada, ordenada y valorada de los elementos que componen el patrimonio de una empresa o persona en un momento determinado. Dichos elementos pueden ser: existencias de almacén, maquinaria, instalaciones, edificios, mobiliario, equipos informáticos, papel, bombillas, papeleras, etc.

### 6.1. Software de código abierto para la gestión del inventario

El primer programa del que vamos a hablar es Odoo [20]. Odoo es una solución ERP de código abierto que integra funciones para ventas, CRM, gestión de proyectos, contabilidad, gestión de almacenes e inventarios, fabricación, gestión financiera, ecommerce o tienda online, recursos humanos, y otros. El paquete básico es suficiente para gestionar los procesos de una pequeña o mediana empresa.

Odoo es una poderosa aplicación absolutamente profesional, que integra todos los procesos de la empresa y permite mantener con facilidad el correcto control de todo lo que ocurre en la empresa y su entorno. Se presenta como una alternativa de código abierto a SAP ERP y Microsoft Dynamics.

En las capturas que podemos ver a continuación podemos ver la parte de Odoo correspondiente a la función que nos interesa que es la de Inventario:

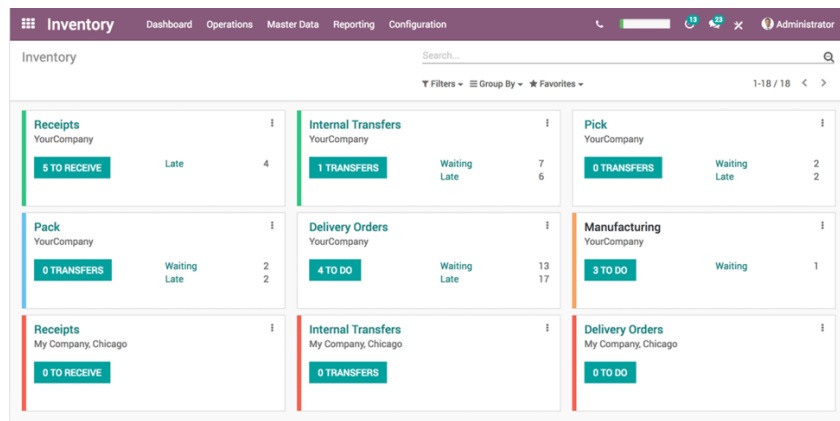


Ilustración 6. Página principal del Inventario

(Página oficial Odoo)

The screenshot shows the Odoo Inventory Internal Transfers list. The table has the following columns: Reference, Destination Location, Partner, Scheduled Date, Source Document, Back Order of, Status, and Batch Picking. The data rows are as follows:

Reference	Destination Location	Partner	Scheduled Date	Source Document	Back Order of	Status	Batch Picking
Picking #1	WH/Output		02/01/2018 09:22:34			Draft	BATCH/00002
Picking #3	WH/Output		02/01/2018 09:22:34			Draft	BATCH/00001
Picking #2	WH/Output		02/01/2018 09:22:34			Draft	BATCH/00002
WH/INT/00003	WH/Stock	Agrolait	02/01/2018 10:42:44	SO102		Cancelled	
WH/INT/00002	WH/Quality Control	Agrolait	02/01/2018 10:42:44	SO102		Cancelled	
WH/INT/00004	WH/Quality Control		02/05/2018 09:27:40	PO00031		Waiting Another Operation	
WH/INT/00005	WH/Stock		02/05/2018 09:27:40	PO00031		Waiting Another Operation	
WH/INT/00007	WH/Stock		02/01/2018 10:42:44			Waiting Another Operation	
WH/INT/00006	WH/Quality Control		02/01/2018 10:42:44			Waiting Another Operation	
WH/INT/00011	WH/Stock		02/01/2018 12:31:33	PO00055		Waiting Another Operation	
WH/INT/00010	WH/Quality Control		02/01/2018 12:31:33	PO00055		Ready	

Ilustración 7. Trazabilidad del Inventario

(Página oficial Odoo)

El segundo de los programas es ERP5 ERP [21]. Es una solución ERP opensource y gratis especializada en empresas y administraciones públicas. ERP5 cubre funciones contables, gestión de relaciones con el cliente CRM, comercio, gestión de almacenes e inventarios, envíos y logística, facturación, gestión de recursos humanos, diseño de productos, producción y gestión de proyectos.

En las capturas que podemos ver a continuación podemos ver la parte de ERP5 correspondiente a la función que nos interesa que es la de Inventario:

Ilustración 8. Vista I del Inventario

(Página oficial ERP5)

Ilustración 9. Vista II del Inventario

(Página oficial ERP5)

El tercer programa es ERPNext [22]. Este programa es un ERP opensource muy simple creado para PYMES. ERPNext incluye módulos de contabilidad, gestión de inventarios, manufacturas, ventas, POS, compras, gestión de recursos humanos y gestión de proyectos. De momento el CRM es muy básico.

En la captura que podemos ver a continuación podemos ver la parte de ERPNext correspondiente a la función que nos interesa que es la de Inventario:

ERPNext > Stock > Purchase Receipt

Search or type a command (Ctrl + G)

Demo User

**Eagle Hardware** Submitted

PREC-00053

Menu Cancel

Comments 0

Make Purchase Invoice Stock Ledger Accounting Ledger

ASSIGNED TO: Assign +

ATTACHMENTS: Attach File +

TAGS: Add a tag...

SHARED WITH: +

Administrator edited this 4 months ago

Administrator created this 4 months ago

Supplier: Eagle Hardware

Date: 11-11-2014

Posting Time: 10:10:37.715678

Time at which materials were received:

Items	Qty	Rate	Amount
1 Base Bearing Plate	2 Nos	\$ 20.00	\$ 40.00
2 Base Bearing Plate	2 Nos	\$ 20.00	\$ 40.00
Total			\$ 80.00

Detailed Breakup of the totals

Taxes and Charges Added

Ilustración 10. Página del inventario

(Página oficial ERP5)

El cuarto programa es Compiere [23]. Y es uno de los sistemas opensource pioneros para empresas. Actualmente, se distribuye como un ERP basado en “la nube”. Integra funcionalidades de gestión, abastecimiento, almacenes e inventarios, y contabilidad. Y puede ser utilizado como un ERP en el canal minorista.

En la captura que podemos ver a continuación podemos ver la parte de Compiere correspondiente a la función que nos interesa que es la de Inventario:

Physical Inventory Search > Inventory Count

Inventory Count 1 / 1

Tenant: GardenWorld Organization: HQ

Document No: 10000000

Description:

Warehouse: HQ Warehouse Perpetual Inventory

Movement Date: 06/03/2008 Document Type: Material Physical Inventory

Create Inventory Count List Update Quantity

Reference

Project: Campaign:

Status

Approved Approval Amount: 0.00

Document Status: Drafted Complete

Ilustración 11. Página del inventario

(Página oficial Compiere)

El quinto programa es xTuple [24]. xTuple era llamado anteriormente OpenMFG y es una solución opensource que integra funciones de contabilidad, ventas, gestión de

relaciones con clientes CRM, compras, definición de productos, inventarios, producción, planificación, etc. La aplicación se distribuye en dos versiones, instalable en servidor o accesible en “la nube”.

En la captura que podemos ver a continuación podemos ver la parte de xTuple correspondiente a la función que nos interesa que es la de Inventario:

Item Number	Description	Site	LT	QOH	Allocated	Unallocated	On Order	Reorder Lvl.	OUT Level	Available
HUB1	Hubcap Type 1 Cars	WH1	1	3638.00	0.00	3638.00	0.00	0.00	0.00	3638.00
RBUMPI	Tough Truck Body Type 1 T...	WH1	3	1490.00	0.00	1490.00	0.00	100.00	1000.00	1490.00
REPAIR1	Repair Type 1 - Truck Job L...	WH1	5	0.00	0.00	0.00	0.00	0.00	0.00	0.00
RTRUCK1	Red Tough Truck Collectors	WH1	5	0.00	0.00	0.00	0.00	0.00	0.00	0.00
SHEET1	Sheet Metal Type 1 Cars - ...	WH1	10	1080.00	0.00	1080.00	0.00	25.00	100.00	1080.00
SHSCRAP1	Scrap Sheet Metal Breeder ...	WH1	1	3777.00	0.00	3777.00	0.00	0.00	0.00	3777.00
STOCKCAR1	Classic Race Car With Log...	WH1	1	107.00	0.00	107.00	0.00	0.00	0.00	107.00
STRUCK1	Collectors Autographed Sl...	WH1	7	6.00	0.00	6.00	0.00	3.00	0.00	6.00
TBODY1	Tough Truck Body Type 1 T...	WH1	1	3077.00	100.00	2977.00	0.00	100.00	1000.00	2977.00
TBOX1	Product Box Type 1 Produc...	WH1	1	0.00	0.00	0.00	0.00	0.00	0.00	0.00
TGCOAT-G	Gloss Coat Finish	WH1	5	197.00	0.00	197.00	0.00	10.00	100.00	197.00
TDECAL-F	FASCAR Racing Decal	WH1	7	9298.00	0.00	9298.00	0.00	1000.00	10000.00	9298.00
TDECAL-P	PUSCH Racing Decal	WH1	7	7703.00	0.00	7703.00	0.00	500.00	5000.00	7703.00
TINSERT1	Packaging Insert Type 1 Ins...	WH1	1	2515.00	0.00	2515.00	0.00	100.00	0.00	2515.00
TKIT1	Truck Kit Type 1 Truck Kit	WH1	1	0.00	100.00	0.00	0.00	0.00	0.00	-100.00
TWHEEL1	Truck Wheel Type 1 Truck ...	WH1	1	6520.00	400.00	6120.00	0.00	400.00	4000.00	6120.00
WTRUCK1	White Tough Truck Collect...	WH1	5	300.00	100.00	200.00	100.00	0.00	0.00	300.00
YPAIN1	Yellow Paint 1 Yellow Pain...	WH1	1	919.13	1.00	919.13	0.00	10.00	100.00	919.13
YPAIN17	Yellow Neon Paint 2 Yellow...	WH1	7	53.99	0.00	53.99	0.00	10.00	50.00	53.99

Ilustración 12. Página del inventario

(YouTube)

El último programa del que vamos a hablar y que se puede encontrar en [25], es GLPI. GLPI es una completa aplicación de código abierto para gestionar el inventario. La aplicación está basada en PHP, MySQL y Apache, por lo que tendremos una administración vía navegador web que nos ayudará con la gestión diaria de nuestra base de datos de inventario, lo que además facilitará la tarea de acceso desde cualquier equipo de nuestra empresa sin necesidad de tener que estar físicamente delante del equipo que tiene instalada la aplicación.

Entre las principales características de GPLI podemos destacar las siguientes:

- Inventario de los equipos, con posibilidad de incluir componentes de hardware como discos duros, y otros componentes de hardware.



- Inventario de periféricos asociados a los equipos, ya sean monitores, ratones, teclados o altavoces, impresoras, etc.
- Inventario de red donde podremos establecer todos los criterios de conexión de nuestros equipos, IP, dirección MAC de la tarjeta de red, VLAN's configuradas.

Además, nos permite incluir datos administrativos como pueden ser periodos de validez de las licencias de software, garantías y tiempos de caducidad de las mismas, o datos de ubicación de los equipos, para tener controlada su ubicación en esta o aquella oficina. Una opción muy útil para empresas con varias sedes.

En la captura que podemos ver a continuación podemos ver la parte de GLPI correspondiente a la función que nos interesa que es la de Inventario:

Name	Entity	Number	Status	Manufacturer	Serial Number	Type	Model	OS	Location	Last update	Contact
computers 0-0	Root entity	num 1		DELL	6midvha89cw	Serveur	Assemble	Windows XP Pro SP2	lieu 1 > s-lieu 0 > ss-lieu 0	2008-03-25 20:43:54	contact 0
computers 0-1	entity 0		Reparation	DELL	6jovgar2td1	Serveur	Assemble	Windows XP Pro SP2	lieu 0 > s-lieu 0 > ss-lieu 0	2008-03-25 20:43:58	contact 0
computers 0-2	entity 1			DELL	df6nmawintg	Serveur	Assemble	Windows XP Pro SP2	lieu 1 > s-lieu 1	2008-03-25 20:44:03	contact 0
computers 0-3	entity 1 > s-entity 0		Reparation	DELL	5n0k25dq5l	Serveur	Assemble	Windows XP Pro SP2	lieu 0 > s-lieu 0 > ss-lieu 1	2008-03-25 20:44:07	contact 0
computers 0-4	entity 2 num 0		Reparation	DELL	v20wtz84knv	Serveur	Assemble	Windows XP Pro SP2	lieu 0 > s-lieu 0 > ss-lieu 0	2008-03-25 20:44:12	contact 0
computers 0-5	entity 2 > s-entity 0		Reparation	DELL	29dabcfzyl	Serveur	Assemble	Windows XP Pro SP2	lieu 1	2008-03-25 20:44:17	contact 0
computers 1-0	Root entity	num 0		DELL	fpq9923iso	Serveur	Assemble	Windows XP Pro SP2	lieu 1 > s-lieu 0 > ss-lieu 0	2008-03-25 20:43:54	contact 1
computers 1-1	entity 0 num 1		Reparation	DELL	1sivtd9k2o	Serveur	Assemble	Windows XP Pro SP2	lieu 0 > s-lieu 0	2008-03-25 20:43:58	contact 1
computers 1-2	entity 1 num 1		Reparation	DELL	7pygl7i9cj	Serveur	Assemble	Windows XP Pro SP2	lieu 0 > s-lieu 0	2008-03-25 20:44:03	contact 1
computers 1-3	entity 1 > s-entity 0	num 0		DELL	rv5fplvxms	Serveur	Assemble	Windows XP Pro SP2	lieu 0 > s-lieu 0 > ss-lieu 0	2008-03-25 20:44:07	contact 1
computers 1-4	entity 2 num 0		Reparation	DELL	unmgko74cq4	Serveur	Assemble	Windows XP Pro SP2	lieu 0 > s-lieu 1 > ss-lieu 0 > sss-lieu 0 >	2008-03-25 20:44:12	contact 1

Ilustración 13. Página del inventario

(Página oficial GLPI)

## 6.2. Conclusión

Como conclusión de esta parte, decir que, como hemos podido observar hay una gran variedad de programas de código abierto para la gestión de inventarios y la mayoría de

ellos tienen otras muchas opciones a parte de la gestión de inventarios por lo que posiblemente nos ayuden a mejorar otras partes de la empresa, aunque esto no lo vamos a saber hasta pasada la auditoría.

Aunque todos los programas son interesantes, los que posiblemente más ayuda nos proporcionarían, serían GLPI o Odoo por las características que tienen.

## 7.- Antecedentes

En este apartado del Trabajo de Fin de Grado se va a hablar sobre la asociación que va a ser nuestro caso de estudio, más detalladamente que en el apartado de introducción, para así poder entender mejor la asociación y poder hacer un mejor trabajo.

APSA es una asociación sin ánimo de lucro creada en el año 1962, y declarada de utilidad pública en 1970, que desarrolla una labor de atención integral a las personas con discapacidad o riesgo de padecerla de la provincia de Alicante. Fruto de su dilatada trayectoria, la asociación ha desarrollado diversos programas complementarios entre sí con el único objetivo de mejorar la calidad de vida de sus usuarios durante todo el ciclo de vida. Dichos programas son de prevención, atención temprana, educación, salud, formación y vivienda, orientados a facilitar su inclusión social y laboral.

El Grupo APSA está compuesto por la Asociación APSA y sus tres centros especiales de empleo: Avícola Aguamarga, Limencop y Terramar. Atiende a alrededor de 2000 personas al año en diversas localidades de la provincia de Alicante. Para ello, cuenta con más de 350 trabajadores, de los cuales más de 200 son personas con discapacidad.

La estructura corporativa está formada por profesionales remunerados y voluntarios. Y la financiación de esta asociación sale de los socios, la venta de servicios, las aportaciones del gobierno, entidades internacionales y de donaciones privadas de empresas y/o particulares. En cuanto a los gastos de APSA podemos decir que destina el 90% de su presupuesto al funcionamiento y mantenimiento de la estructura y el resto a proyectos. Por lo tanto, el mayor objetivo de APSA para poder llegar al ideal de ONG y ser reconocidos es: “CONSEGUIR MAYOR FINANCIACIÓN”.

Para poder entender en qué situación se encuentra la asociación vamos a poner el DAFO de esta.

Las fortalezas son:

- Capacidad para gestionar y aprovechar el mercado y la responsabilidad social (RSC) de las empresas y entidades.

- Nivel técnico elevado de los tratamientos, intervenciones y actividades de los diferentes centros y servicios en relación al resto de asociaciones.
- Existencia de una dirección técnica que da coherencia e impulsa la mejora organizativa emprendida durante los últimos años.
- Puesta en marcha de un equipo directivo que coordina y alinea una organización con centros y servicios muy diferentes.
- Implicación y motivación de los profesionales, familias y miembros de la Junta Rectora con los fines de la entidad y las personas con discapacidad.
- Existencia de centros y departamentos como Servicios Generales, Comunicación y Formación y Proyectos que otorgan un mayor nivel cualitativo y técnico a la actividad de la asociación.
- Red de alianzas, clientes y contactos institucionales amplia.
- Intervención en todo el ciclo biográfico de la persona con discapacidad intelectual o del desarrollo (PDID).
- Buena reputación de la marca APSA.
- Modo de gestionar los ERE's, la crisis de tesorería en el grupo y la negociación del convenio con el esfuerzo de todos y el modelo de concertación con los comités nos ha consolidado como asociación.
- Capacidad de gestión sostenida en el tiempo.
- Dilatada experiencia tras cincuenta y tres años de historia.
- Ámbito de actuación provincial.

Las oportunidades son:

- Cambio político a nivel autonómico y local favorable a la gestión de las entidades no lucrativas en la acción social.
- Redacción de una nueva Ley de SS.SS.: si se materializa una mayor dificultad del sector lucrativo para acceder a la acción social, puede favorecer licitaciones y gestión de servicios por parte de las entidades no lucrativas (ENL's).
- El hecho de convertirnos en los “especialistas en discapacidad” ante la Consellería, determinados ayuntamientos y empresas. Venta de conocimiento y consultoría.

- “Desembarco” del Grupo APSA en otras comarcas, dado el estancamiento de iniciativas y de nivel técnico de algunas asociaciones.
- Nuevos segmentos de clientes.
- Alianzas.

Las debilidades son:

- Base asociativa pequeña en relación al tamaño organizativo.
- Poca cultura de evaluación y falta de sistemas de indicadores para medir los resultados de los centros.
- Necesidad de una evaluación del desempeño de los directivos para extenderla después al resto de profesionales.
- Carecemos de estrategia explícita a largo plazo como organización.
- Aunque estamos avanzando mucho debemos seguir profundizando en el ciclo de planificación anual, integrando los niveles técnicos, de infraestructuras y económico.
- Necesidad de consolidar la formación continua de los profesionales.
- Cabe revisar las necesidades reales de dotación de personal para la atención a PDID en los centros.
- Diversos aspectos organizativos y de la política de personas están todavía implantándose, tales como Prevención de Riesgos Laborales, LOPD y otros.
- APSA no ha sabido desplegar toda la potencialidad del voluntariado: entre otras razones porque gestión del voluntariado en sentido estricto se lleva a cabo sólo desde hace unos años.
- Falta de inversión sistemática y planificada en los edificios e instalaciones con la consiguiente depreciación y deterioro de dichos activos.
- Equipamiento tecnológico obsoleto y disfuncional.
- Endeudamiento ya existente conduce a un esfuerzo financiero importante e ineludible durante los próximos años.
- Poca participación de las PDID en los centros, servicios y en la asociación.

- El posicionamiento de APSA reside en una imagen fundamentalmente benéfica (en el mejor sentido del término) y apenas en lo técnico, lo socio-comunitario o lo reivindicativo.
- No se comparten las buenas prácticas de los distintos centros y servicios.
- Poca utilización del benchmarking como herramienta de mejora. Dado que están a un nivel distinto que las asociaciones de su entorno y el sector no tiene marcos de encuentro ni indicadores para ser comparados, corremos el riesgo de la endogamia.
- No obtención del certificado de Fundación Lealtad.
- Nula presencia en los foros federativos estatales.

Las amenazas son:

- Aparición en el entorno comarcal y provincial de entidades que trabajan con la discapacidad; con un objetivo poco claro, pero con un marketing muy incisivo.
- Competencia feroz de servicios privados en ciertos tramos de edad, sobre todo en etapa educativa.
- Marco económico todavía en crisis y falta de dinamismo. La comunidad autónoma es una de las más afectadas por la crisis a nivel económico e institucional.
- Deficiente gestión autonómica y local en los servicios sociales y sanitarios durante las últimas legislaturas que ha dejado una herencia complicada.
- Enorme deuda autonómica que obstaculizará cualquier planteamiento del nuevo gobierno y puede volver a ocasionar una crisis de tesorería, dado que la principal fuente de financiación de la asociación es la Generalitat.
- Pérdida de terreno por parte de APSA frente a entidades por dejar pasar oportunidades y necesidades a cubrir.

Para seguir entendiendo la Asociación APSA queremos poner los pilares en los que se basa su gestión, que son cinco:

1. Calidad: APSA dispone de la certificación ISO 9001:2008 y mejora de forma continua la calidad de sus servicios.

2. Transparencia: su gestión es transparente. Sus cuentas son auditadas anualmente y publican su memoria de actividades, entre otras actuaciones.
3. Investigación: colaboran con universidades y fundaciones en la investigación para la mejora de la calidad de vida de las personas con discapacidad.
4. Desarrollo: APSA desarrolla su cartera de servicios para responder a las necesidades de los socios. Asimismo, amplía y mejora la formación de sus trabajadores.
5. Innovación: incorporan nuevos servicios e intervenciones basadas en evidencia científica para lograr los mejores resultados posibles en nuestras intervenciones.

En cuanto a las sedes o delegaciones con las que trabaja APSA son 10, aunque la sede Central se encuentra en Alicante (Avd. Salamanca) y se ocupa sobre todo del desarrollo infantil y la atención temprana (CDIAT). Otra de las sedes se encuentra en San Vicente y se ocupa del desarrollo infantil y la atención temprana, así como es un centro de recursos y apoyo escolar (CRAE). La tercera área educativa se encuentra en La Vila Joiosa y es un CDIAT y un CRAE, como la de San Vicente. Después encontramos el CRAE con el Servicio de Ocio y las Actividades Artísticas en Alicante (C/Zarandietta). En Alicante (C/García Morato) también podemos encontrar la actividad artística de Psicoballet con monitores. En Elche podemos encontrar otra sede con un centro de formación permanente (CFP) o como APSA denomina Camí Obert y un CRAE. En la siguiente sede de Alicante (C/Catedrático Jaume Mas i Porcel) podemos encontrar otro Camí Obert. Y finalmente, podemos encontrar un CFP Camí Obert en Alfàs del Pi. En la Partida Aguamarga de Alicante podemos encontrar el área de empleo y el centro ocupacional Terramar. Y por último el área residencial y centro ocupacional de San Juan.

Con el objetivo de crear recursos especializados que se complementen entre sí y que permitan a la persona con discapacidad mejorar su calidad de vida, APSA estructura su cartera de servicios en cuatro áreas: Educativa, de Transición a la Vida Adulta, Vida Adulta y Tercera Edad.

- La Etapa Educativa comprende desde el nacimiento hasta los 16 años de edad. Se orienta al apoyo del niño con discapacidad o riesgo de presentarla y su familia,

desde la educación secundaria obligatoria. Cuenta con el CDIAT, con el CRAE y diversos servicios complementarios.

- La etapa de Transición a la Vida Adulta se orienta a jóvenes con discapacidad con edades entre los 16 y los 26 años de edad. Prepara al joven para su inclusión social, así como para su incorporación a una ocupación o un empleo. Cuenta con los Centros Camí Obert y varios servicios que cubren las necesidades de este periodo.
- La etapa de Vida Adulta se orienta a personas con discapacidad mayores de 26 años. Ofrece servicios de intermediación laboral, ocupación o empleo. Cuenta con el Centro de Orientación, Formación y Asesoramiento Laboral (COFAL), el Centro Ocupacional Terramar, tres centros especiales de empleo (Avícola Aguamarga, Limencop y Terramar) y diversos servicios.
- En la etapa de la Tercera Edad se ofrecen los apoyos necesarios en los últimos años de vida de la persona con discapacidad. Ofrece, entre otros, servicios de apoyo domiciliario, apoyo psicológico, ocio y deporte, etc. orientados a personas de más de 65 años.

Hasta ahora la actividad de la asociación ha sido desarrollada mediante métodos y procedimientos tradicionales de atención y apoyo, utilizando la TI como herramienta primero administrativa y poco a poco la han ido introduciendo dentro de sus metodologías de tratamiento.

Ahora surge una oportunidad con la Catedra Institucional “Aguas de Alicante Inclusión Social”, cátedra innovadora que actúa en el campo de la inclusión social, mediante la cual la asociación ve la oportunidad de utilizar la TI como parte de su cadena de valor, eso significa que ahora va a poder hacer cosas que antes no podía como por ejemplo cursos online o atención remota, entre otras.

Por lo que, para finalizar este apartado de antecedentes, vamos a comentar brevemente el proyecto llamado e-apsa que tiene en marcha la asociación APSA, a través de la citada Cátedra y que vamos a tener que tener en cuenta a la hora de la auditoría.



El proyecto consiste en el desarrollo y puesta en marcha de una plataforma online con los siguientes fines:

- a) La formación, bajo la modalidad de e-learning o b-learning, de profesionales (tanto de APSA como externos) en el ámbito de la atención a personas con discapacidad o riesgo de presentarla y sus familias o tutores legales.
- b) La formación y orientación de personas con discapacidad intelectual (e-learning, b-learning, e-guidance, e-counseling),
- c) La formación y orientación a familias (e-learning, b-learning, e-guidance, e-counseling),
- d) Complementar la atención presencial con tutorías y asesoramiento virtuales (e-counseling),
- e) Atender al socio mediante un repositorio de recursos,
- f) Crear un foro para la interacción de familias o usuarios.

El proyecto surge como reacción a una serie de necesidades que se han detectado en la atención a sus grupos de interés, y que se enumeran a continuación:

- a) Dificultad de las familias para acudir a reuniones individuales o en grupo en las sedes de APSA.
- b) Tras la aplicación de diversos programas de alfabetización digital de personas con discapacidad intelectual, existe la necesidad de diseñar servicios digitales específicamente para ellos y sus propias necesidades.
- c) Necesidad de sistematizar la información sobre APSA y ofrecérsela al socio en un único repositorio.
- d) Necesidad de sistematizar y compilar todas las actuaciones relativas a la formación de trabajadores que se realizan en la entidad. Determinados cursos y sus contenidos se pierden puesto que no se ha sistematizado su compilación y una forma de ofrecerlos permanentemente como estrategia de formación permanente de nuestro personal.
- e) Necesidad de que las familias puedan comunicarse con las terapeutas y psicólogas mediante recursos a distancia.

- f) Necesidad de poner en contacto a familias entre sí, especialmente aquellas que comparten circunstancias similares en un momento determinado, ofreciendo recursos a distancia utilizando las nuevas tecnologías.

En conjunto, la incorporación de la metodología de e-learning, b-learning y e-counseling supondrá una nueva forma de trabajo en APSA. Les abre enormes posibilidades de mejora de la eficacia y de la eficiencia en su trabajo. Por ejemplo, permite que los profesionales puedan atender a las familias sin tener que necesariamente coincidir en un espacio y tiempo concretos. Asimismo, facilitará la acumulación progresiva de servicios y contenidos, lo cual favorecerá que, en poco tiempo, dispongan de una verdadera biblioteca de cursos, recursos y servicios a disposición de los diversos grupos de interés.

Este cambio de forma de trabajar, tendiendo hacia la TI es la que obliga y justifica el realizar una auditoría TI, ya que la empresa va a hacer una fuerte inversión tanto organizacional como económica para apostar por la oferta de servicios digitales, que tengan un mayor alcance, un mayor impacto y aumenten la cadena de valor de la asociación. Antes de crear nuevos servicios, es necesario analizar los actuales, la TI desplegada, y alinear los servicios existentes junto con los nuevos objetivos de negocio y la TI que tendremos que crear.

## 8.- Objetivos

Como ya se ha comentado en la parte de Introducción, el objetivo principal de este Trabajo de Fin de Grado será abordar las cuestiones relativas a la realización de una Auditoría TI en una empresa real que tiene previsto introducirse en el mundo de los servicios digitales.

Para cumplir el objetivo principal, se definen los siguientes sub-objetivos específicos:

- El primer sub-objetivo es hacer un estudio de cómo realizar una auditoría en TI.
- El segundo sub-objetivo es diseñar un procedimiento junto con las herramientas necesarias para hacer la auditoría TI.
- El tercer sub-objetivo es llevar a cabo la auditoría en la Asociación APSA, junto con la emisión del informe final de recomendaciones y conclusiones extraídas.
- El cuarto y último sub-objetivo es ayudar a implantar las conclusiones extraídas del informe auditor.

## 9.- Plan auditor

En este apartado correspondiente al Plan auditor, vamos a hablar sobre el plan auditor que se va a seguir para realizar la auditoría en la Asociación APSA.

El plan auditor es la guía específica que se debe seguir al realizar una auditoría. Esta guía sirve de ayuda al auditor para saber que debe hacer en cada parte de la auditoría y de esa manera ayuda a evitar malentendidos con el cliente. Para crear el plan auditor, vamos a tomar como base los trabajos que podemos encontrar en 5.1 Guía para realizar una auditoría informática paso a paso, 5.2 Auditoría Informática Planificación, 5.3 Metodología para realizar una auditoría y 5.4 Pasos para realizar una auditoría en sistemas informáticos, pero además añadiremos ciertos aspectos relacionados con otras cosas que nos resulten de interés para realizar la auditoría. A partir de esto, vamos a diseñar nuestro propio plan auditor el cual estará dividido en etapas y cada una de estas en una serie de pasos.

### 9.1.- Etapa de análisis

La primera etapa es la correspondiente al análisis. Este paso es imprescindible porque no todas las empresas tienen los mismos objetivos cuando encargan una auditoría informática y además no todas las empresas son iguales. Por tanto, el primer paso de esta parte correspondiente al análisis será identificar el origen de la auditoría, el segundo paso será determinar los objetivos que se tienen, el tercer paso será conocer la empresa y, el cuarto será hacer un inventario de todos los aspectos concernientes a los sistemas y usos informáticos en la empresa, con lo que será inevitable una estrecha colaboración entre los altos cargos, los auditores y los técnicos informáticos.

De manera más extensa y más específica los puntos que hemos comentado anteriormente se podrían dividir en:

1. Identificar el origen de la auditoría: En este primer paso se debe determinar por qué surge la necesidad o inquietud de realizar una auditoría. Las preguntas que se deben

contestar ¿de dónde?, ¿por qué?, ¿quién? o ¿para qué? se quiere hacer la evaluación de algún aspecto de los sistemas de la empresa.

2. Determinar los objetivos de la auditoría: En este segundo paso, las personas que realizan la auditoría han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar. Deben comprender los deseos y pretensiones del cliente, de forma que las metas fijadas puedan ser cumplidas.
3. Conocer la empresa: En este tercer paso, se requiere obtener información general sobre la organización.

El auditor debe conocer lo siguiente:

- Organigrama: El organigrama expresa la estructura oficial de la organización a auditar. Si se descubriera que existe un organigrama fático diferente al oficial, se pondrá de manifiesto tal circunstancia.
  - Departamentos: Se entiende como departamento a los órganos que siguen inmediatamente a la Dirección.
  - Áreas de la cartera de servicios: Serán las áreas en las que se estructura su cartera de servicios.
  - Sedes: Las sedes son las distintas delegaciones o locales que tiene la organización.
  - Número de puestos de trabajo: El equipo auditor comprobará que los nombres de los puestos de trabajo de la organización corresponden a las funciones reales distintas.
  - Número de personas por puesto de trabajo: Es un parámetro que los auditores informáticos deben considerar. La inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.
  - Otros: Se conocerá también otros datos de interés para conocer la empresa, como cuál es la actividad de la empresa, etc.
4. Inventario de sistemas y usos informáticos: En este cuarto paso, se quiere conocer el entorno en el que va a desenvolverse la auditoría obteniendo información sobre los sistemas y los usos informáticos de la organización. Para ello se realizará una

visita preliminar al área de informática con la que se tendrá un primer contacto con el personal asignado a dicha área, conociendo así:

- La situación geográfica de los sistemas: Se determinará la ubicación geográfica de los distintos centros de proceso de datos en la empresa.
- Responsables TI: Se verificará la existencia de responsables en cada uno de los distintos centros de proceso, así como el uso de los mismos estándares de trabajo.
- Arquitectura y configuración de hardware y software: Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado.
- Inventario de hardware y software: El auditor recabará información escrita, de donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a hardware figurarán las CPUs, unidades de control local y remotas, periféricos de todo tipo, etc.
- Comunicación y redes de comunicación
- Las medidas de seguridad y otros aspectos sobre que problemáticas que se presentan en el área auditada.
- Aplicaciones bases de datos y ficheros: Se conocerá el tamaño y características de las bases de datos, clasificándolas en relación y jerarquías.

## 9.2.- Etapa de planificación

La segunda etapa es la planificación y su contenido es el siguiente: cuando tenemos claros los objetivos de la auditoría informática y demás cosas de la etapa de análisis, así como los usos más habituales dentro de la empresa, planificamos nuestra auditoría a través de herramientas de análisis. En esta etapa de la auditoría determinaremos los puntos que serán evaluados, haremos el diseño de métodos, técnicas y procedimientos necesarios para llevarla a cabo y solicitaremos los documentos que servirán de apoyo para la ejecución, terminando con la elaboración de la documentación de los planes, programas y presupuestos para llevarla a cabo y la asignación de los recursos para realizar la auditoría.

De manera más extensa y más específica los puntos que hemos comentado anteriormente se podrían dividir en:

1. Determinar los puntos que serán evaluados: Una vez determinados los objetivos de la auditoría se deben determinar los aspectos que serán evaluados, y para esto se debe considerar aspectos específicos del área informática y de los sistemas computacionales tales como: la gestión administrativa del área informática y el centro de cómputo, el cumplimiento de las funciones del personal informático y usuarios de los sistemas, los sistemas en desarrollo, la operación de los sistemas en producción, protección de las bases de datos, datos confidenciales y accesos a las mismas, protección de las copias de seguridad y la restauración de la información, seguridad de los servidores, entre otros aspectos.

2. Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría: En este punto se determina la documentación y medios necesarios para llevar a cabo la revisión y evaluación en la empresa, seleccionando o diseñando los métodos, procedimientos o herramientas, las cuales suelen ser cuestionarios, checklists, entrevistas o trazas y/o huellas, visitas y otros instrumentos necesarios para realizar la auditoría.

3. Elaborar planes y programas para realizar la auditoría: Para realizar la planeación formal de la auditoría informática y de sistemas, en la cual se concretan los planes y programas para llevarla a cabo se debe elaborar los documentos formales para el desarrollo de la auditoría, donde se delimiten las etapas, eventos y actividades y los tiempos de ejecución para el cumplimiento del objetivo.

Algunos de los aspectos a tener en cuenta serán: Las actividades que se van a realizar, los responsables de realizarlas, los recursos materiales y los tiempos; el flujo de eventos que sirven de guía; la estimación de los recursos humanos, materiales e informáticos que serán utilizados; los tiempos estimados para las actividades y para la auditoría; los auditores responsables y participantes de las actividades; otras especificaciones del programa de auditoría.

4. Asignar los recursos y sistemas computacionales para la auditoría: Finalmente, se debe asignar los recursos que serán utilizados para realizar la auditoría. Con la asignación de estos recursos humanos, informáticos, tecnológicos y de cualquier otro tipo se llevará a cabo la auditoría.

### 9.3.- Etapa de ejecución

La tercera etapa es la ejecución de la auditoría. En esta etapa se ejecuta la auditoría, es decir, primeramente, se decide en qué áreas se va a realizar la auditoría, ya que, la auditoría informática general se realiza por áreas generales o por áreas específicas; sabiendo que, si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos. Una vez decididas las áreas se realiza esta, que está determinada por las características propias, los puntos elegidos y los requerimientos estimados en la planificación. Para realizarla se utilizará toda la información que se ha adquirido en los puntos anteriores, así como se utilizarán los métodos y herramientas que se han propuesto y decidido en la etapa de planificación.

Los pasos concretos en esta etapa de ejecución de la auditoría son:

1. Ejecutar las herramientas de análisis. Enviar cuestionarios, aclarar dudas, realizar las entrevistas y cualquier otra herramienta, asegurando recoger de la forma más completa toda la información prevista necesaria.
2. Revisión de los materiales. Revisar la completitud de los cuestionarios, entrevistas y otros materiales, generar lista de dudas y aclaraciones y enviar de nuevo cuestiones a los actores (punto 1).
3. Emitir conformidad de ejecución. Dictaminar que toda la información que se desea recopilar está completa o que ya no es posible recoger más.



## 9.4.- Etapa de dictamen

La cuarta, y final, etapa es la de dictamen de la auditoría que es el resultado final de la auditoría, donde se presentan los siguientes puntos: elaboración del informe de las situaciones que se han detectado, la elaboración del dictamen final y la presentación del informe de auditoría de la siguiente manera:

1. Analizar la información y elaborar un informe de las situaciones detectadas: Junto con la detección de las oportunidades de mejoramiento se debe realizar el análisis de los papeles de trabajo y la elaboración del borrador de las oportunidades detectadas, para ser discutidas con los auditados, después se hacen las modificaciones necesarias y posteriormente el informe final de las situaciones detectadas.

2. Elaborar el dictamen final: El auditor debe terminar la elaboración del informe final de auditoría y complementarlo con el dictamen final, para después presentarlo a los directivos del área auditada para que conozcan la situación actual del área, antes de presentarlo al representante o gerente de la empresa.

Una vez comentadas las desviaciones con los auditados, se elabora el informe final, lo cual es garantía de que los auditados ya aceptaron las desviaciones encontradas y que luego se llevan a documentos formales.

3. Elaborar el dictamen formal o informe de auditoría: El último paso de esta metodología es presentar formalmente y el dictamen de la auditoría al más alto de los directivos de la empresa donde se informa de los resultados de la auditoría. Tanto el informe como el dictamen deben presentarse en forma resumida, correcta y profesional. La presentación de la misma se hace en una reunión directiva y por eso es indispensable usar un lenguaje claro tanto en el informe como en la exposición del mismo. El informe debe contener los siguientes puntos: la carta de presentación, el dictamen de la auditoría, el informe de situaciones relevantes y los anexos y cuadros estadísticos.

Al elaborar el dictamen formal se hace tomando en cuenta el informe comentado a los directivos, junto al informe de hallazgos o desviaciones y los documentos de trabajo de

cada uno de los auditores. La integración del dictamen y el informe final de auditoría deben ser elaborados con la máxima perfección, tratando de evitar errores. También deben contener de manera clara y concreta, las desviaciones detectadas en la evaluación.

Como podemos observar, nuestro plan auditor consta de cuatro etapas que son análisis, planificación, ejecución y dictamen. En cada una de las etapas se describe los pasos que se van a realizar y que se debe hacer en cada paso. Como ya hemos descrito en el punto 7.- Antecedentes, un conocimiento de la empresa, solo lo tendremos que volver a redactar en la parte correspondiente.

## 10.- Auditoría (resultados)

Después de tener claro cuál va a ser nuestro Plan Auditor, vamos a pasar a realizar todas sus etapas y sus pasos, por lo que en este apartado vamos a realizar la Auditoría en sí.

### 10.1. – Etapa de análisis

Los objetivos de la Asociación APSA son tanto mantener sus actuales servicios TI como incorporar los nuevos servicios TI derivados del proyecto de la Cátedra de Inclusión.

1. Identificar el origen de la auditoría: La necesidad de realizar esta Auditoría TI surge a través de la creación de la Cátedra de Inclusión dirigida por el Vicerrectorado de Responsabilidad Social, Inclusión e Igualdad de la Universidad de Alicante junto con Aguas de Alicante y la Asociación APSA. Puesto que a través de esta Cátedra se va a realizar un importante esfuerzo de innovación TI para ofrecer nuevos servicios y mejorar sus actuales procesos empresariales, ya que este proyecto de innovación persigue la mejora y crecimiento en la oferta de servicios a sus asociados, se realizará una Auditoría TI para poder ver en qué situación se encuentra la Asociación y así determinar que necesidades tienen y que camino deben seguir para conseguir los objetivos anteriormente mencionados.

2. Determinar los objetivos de la auditoría: Los objetivos de esta auditoría son analizar todo lo referente a la TI en la Asociación APSA y aconsejarles sobre las mejoras que deberían hacer si quieren lograr sus objetivos, ya comentados anteriormente.

3. Conocer la empresa/asociación:

- **Organigrama**: En el nivel organizativo más alto de la Asociación APSA se encuentra la Asamblea General de Socios, en el siguiente nivel hay una Junta Rectora junto con una Junta de Apoyo, por debajo se encuentra el Gerente, a continuación, se encuentra la Directora Técnica, después se encuentran los encargados de cada área que son las siguientes: área Educativa, área de Formación, área Residencial, C.O. San Juan y Voluntariado, C.O. Terramar y Calidad y Ocio, área de Empleo, área Infraestructuras y TIC y área Comunicación

y Marketing, en el siguiente nivel se encuentran las Direcciones y Coordinaciones de Centros y Servicios y finalmente, los Equipos Técnicos.



Ilustración 14. Organigrama APSA

(Asociación APSA)

- Departamentos – Servicios - Áreas: En la imagen que se muestra a continuación, podemos ver los distintos departamentos, servicios y áreas de la Asociación APSA:

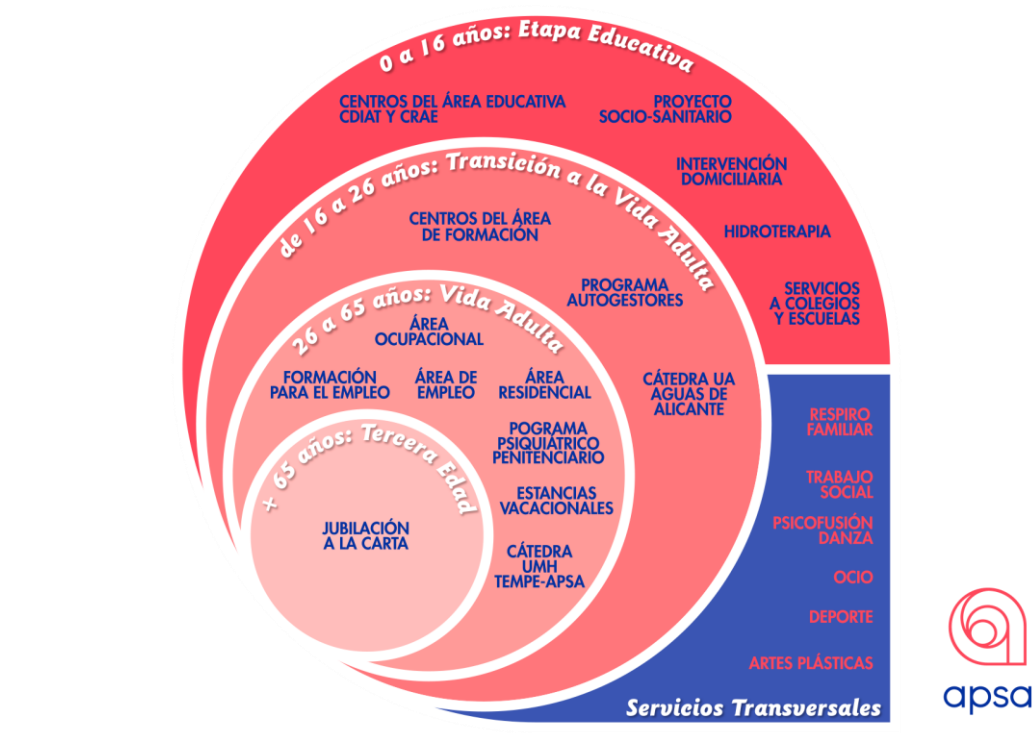


Ilustración 15. Departamentos-Servicios-Áreas APSA

(Asociación APSA)

- **Áreas de la cartera de servicios:**

La Asociación APSA estructura su cartera de servicios en cuatro áreas: etapa Educativa, etapa de Transición a la Vida Adulta, etapa de Vida Adulta y etapa de Tercera Edad.

La Etapa Educativa comprende desde el nacimiento hasta los 16 años de edad. Se orienta al apoyo del niño con discapacidad o riesgo de presentarla y su familia, desde la educación secundaria obligatoria. Cuenta con el CDIAT, con el CRAE y diversos servicios complementarios. Esta etapa educativa contempla actividades según el grupo de edad de las personas:

De 0 a 6 años

- **CDIAT:** se orienta a niños y niñas de 0 a 6 años, con discapacidad o riesgo de presentarla. Ofrece sesiones de 45 minutos de duración una o varias veces a la semana, en horario de mañana o tarde, de lunes a viernes. Estas sesiones pueden incluir uno o varios de los siguientes servicios:

fisioterapia, logopedia, integración sensorial, estimulación basal, terapia ocupacional, hidroterapia, atención temprana, psicomotricidad y atención a familias.

#### De 6 a 16 años

- CRAE: se orienta a niños y niñas de 6 a 16 años, con discapacidad o riesgo de presentarla. Ofrece sesiones de 45 minutos de duración una o varias veces a la semana, en horario de mañana o tarde, de lunes a viernes. Estas sesiones pueden incluir uno o varios de los siguientes servicios: fisioterapia, logopedia, apoyo escolar, aprendizaje de habilidades adaptativas, aprendizaje de habilidades sociales y atención a familias.
- Ocio y deporte: se oriente a niños y niñas de 6 a 16 años, con discapacidad o riesgo de presentarla. Ofrece actividades lúdicas en horario de mañana y tarde y actividades de deporte adaptado en horario de tarde. Cuenta para ello con monitores especializados que organizan diversas actividades recreativas, lúdicas y culturales comunitarias (cine, teatro, exposiciones, excursiones, etc.), actividades vacacionales (viajes y campamentos) y actividades deportivas como natación, fútbol y senderismo.
- Respiro familiar: se orienta a las familias de niños y niñas con discapacidad de 6 a 16 años. Ofrece estancias en fines de semana y puentes además de apoyos puntuales (el monitor se desplaza al hogar) para que los familiares a cargo del niño puedan tener un periodo de descanso.
- Apoyo psicológico: orientado a niños y niñas de 6 a 16 años, con discapacidad o riesgo de presentarla y/o a sus familiares. Ofrece sesiones de orientación y apoyo psicológico con una duración de una hora, bajo cita previa. Su horario es de mañana o tarde.
- Formación en nuevas tecnologías: se orienta a niños y niñas con discapacidad o riesgo de presentarla, de 6 a 16 años a través de cursos en horario de mañana o de tarde en los que se enseña el manejo de recursos tecnológicos como el ordenador y sus programas más habituales

(internet, redes sociales, etc.), teléfono móvil o tabletas. También se ofrece formación orientada a los familiares.

- Actividades artísticas: se orienta a niños y niñas de 6 a 16 años, con discapacidad o riesgo de presentarla. Ofrece actividades de artes plásticas (cerámica, pintura) y escénicas (baile adaptado, acondicionamiento físico, nuevos ritmos), en horario de mañana y tarde.

#### De 0 a 16 años

- Formación a familias: ofrece cursos en horario de mañana o tarde, dirigidos a familiares de personas con discapacidad o riesgo de presentarla. Estos cursos tienen una duración variable y tratan sobre temas de interés para las familias (problemas de conducta, alimentación, sueño, etc.).
- Trabajo social: es un servicio dirigido a las familias de usuarios de APSA o bien a personas externas que solicitan únicamente este servicio. Informa, orienta y acompaña en el proceso de tramitación de recursos (ayudas y becas) y solicitudes. También gestiona las distintas demandas y solicitudes de información.
- Unidad Volante de Apoyo a la Dependencia: se dirige a niños y niñas, con discapacidad o riesgo de presentarla, de 0 a 16 años. Ofrece sesiones de 45 minutos a domicilio, una o varias veces a la semana, de lunes a viernes. Estas sesiones pueden incluir, según sea necesario, los siguientes servicios: fisioterapia, logopedia, terapia ocupacional. De forma complementaria ofrece, además, atención familiar.
- Servicio de Apoyo Educativo (SAE): ofrece apoyos psicopedagógicos y logopédicos en el propio centro escolar a personas con necesidades específicas de apoyo educativo a través de sesiones de intervención de 45 minutos, con una periodicidad semanal y una intensidad variable (1, 2 o 3 sesiones semanales).

La etapa de Transición a la Vida Adulta se orienta a jóvenes con discapacidad con edades entre los 16 y los 26 años de edad. Prepara al joven para su inclusión

social, así como para su incorporación a una ocupación o un empleo. Cuenta con el Centro Camí Obert y varios servicios que cubren las necesidades de este periodo.

#### De 16 a 26 años

- Centro de transición a la vida adulta Camí Obert: se orienta a jóvenes con discapacidad de 16 a 26 años de edad. Ofrece programas formativos de uno o varios cursos de duración, con un amplio horario de formación al día, de lunes a viernes, por la mañana y por la tarde. Esta formación incluye asignaturas como lenguaje, cálculo, formación y orientación laboral (FOL), formación profesional inicial en varias especialidades, destrezas adaptativas (vida personal, en el hogar, en comunidad), etc. Camí Obert desarrolla varios programas de cualificación profesional inicial (PCPI) y ofrece servicios de formación preprofesional, formación continua y atención familiar.
- Ocio y deporte: se orienta a jóvenes de 16 a 26 años con discapacidad. Ofrece actividades lúdicas en horario de mañana y tarde y actividades de deporte adaptado en horario de tarde. Cuenta para ello con monitores especializados que organizan diversas actividades recreativas, lúdicas y culturales comunitarias (cine, teatro, exposiciones, excursiones, etc.), actividades vacacionales (viajes y campamentos) y actividades deportivas como natación, fútbol y senderismo.
- Respiro familiar: se orienta a las familias de niños y niñas, con discapacidad, de 16 a 26 años. Ofrece estancias durante un fin de semana y puentes, además de apoyos puntuales (en los que el monitor se desplaza al hogar) para que los familiares a cargo del niño puedan tener un periodo de descanso.
- Formación en nuevas tecnologías: se orienta a jóvenes con discapacidad o riesgo de presentarla, de 16 a 26 años. También se ofrece cursos en horario de mañana o tarde para aprender a manejar varios recursos tecnológicos: ordenador y sus programas, internet, redes sociales, teléfono móvil, tabletas, etc.



- Unidad Volante de Apoyo a la Dependencia: se dirige a jóvenes con discapacidad o riesgo de presentarla, de 16 a 26 años. Ofrece sesiones de 45 minutos a domicilio, una o varias veces a la semana, de lunes a viernes. Estas sesiones pueden incluir una o varios de los siguientes servicios: fisioterapia, logopedia, terapia ocupacional, cuidado y apoyo al dependiente, programa adultos solos, etc. De forma complementaria ofrece, además, atención familiar.
- Formación a familias: ofrece cursos en horario de mañana o tarde, dirigidos a familiares de personas con discapacidad o riesgo de presentarla. Estos cursos tienen una duración variable y tratan sobre temas de interés para las familias (problemas de comportamiento, estimulación para el desarrollo de las destrezas adaptativas, sexualidad, etc.).
- Trabajo social: es un servicio dirigido a las familias de usuarios de APSA o bien personas que solicitan únicamente este servicio. Se orienta a la gestión de recursos (ayudas y becas) y solicitudes (certificado de discapacidad, reconocimiento de dependencia), atención a demandas, información y asesoramiento.
- Apoyo psicológico: orientado a jóvenes con discapacidad de 16 a 26 años y/o sus familiares. Ofrece, bajo cita previa, sesiones de orientación y apoyo psicológico de una hora de duración. Asimismo, ofrece servicios de diagnóstico y valoración. Su horario es de mañana o tarde.
- Actividades artísticas: se orienta a jóvenes de 16 a 26 años, con discapacidad o riesgo de presentarla. Ofrece actividades de artes plásticas (cerámica, pintura) y escénicas (baile adaptado, acondicionamiento físico, nuevos ritmos), en horario de mañana y tarde.

#### De 18 a 26 años

- Vivienda: se orienta a personas con discapacidad mayores de 18 años. Ofrece alojamiento, manutención y apoyo para la vida independiente a través de diversos servicios: residencia y viviendas tuteladas.

La etapa de Vida Adulta se orienta a personas con discapacidad mayores de 26 años. Ofrece servicios de intermediación laboral, ocupación o empleo. Cuenta con el Centro de Orientación, Formación y Asesoramiento Laboral (COFAL), el Centro Ocupacional Terramar, tres centros especiales de empleo (Avícola Aguamarga, Limencop y Terramar) y diversos servicios.

- COFAL: se orienta a jóvenes con discapacidad a partir de 20 años de edad. Ofrece bolsa de formación y bolsa de empleo para personas que buscan trabajo o para empresarios que desean contratar a trabajadores con discapacidad. El COFAL realiza múltiples cursos de formación para el empleo a lo largo del año, tanto en horario de mañana como de tarde. Esta formación incluye formación profesional específica (en diversas especialidades como, por ejemplo, en auxiliar de comercio) y prácticas no laborales en empresas o centros especiales de empleo. Asimismo, este centro ofrece servicios de formación continua y reciclaje profesional, y formación en nuevas tecnologías.
- Centro Ocupacional Terramar: va dirigido a personas con discapacidad hasta los 65 años. Ofrece programas de ajuste personal y social, así como una formación laboral específica para la transición hacia el empleo. Además, ofrece ocupación para aquellas personas con discapacidad que no pueden acceder a un entorno laboral. Dispone de servicio de transporte y comedor. Su horario es de mañana y tarde.
- Centros especiales de empleo: el Grupo APSA cuenta con tres centros especiales de empleo: Avícola Aguamarga, Limencop y Terramar. Estos centros se orientan a personas con discapacidad en edad laboral y ofrecen trabajo en la modalidad de empleo protegido. Su actividad económica incluye actividades como la limpieza, la conserjería, la reprografía, la encuadernación, el diseño gráfico, auxiliar de comercio, etc.
- Ocio y deporte: se orienta a personas mayores de 26 años, con discapacidad. Ofrece actividades lúdicas y actividades de deporte adaptado con monitores especializados como, por ejemplo: actividades

de ocio y cultura en la ciudad (cine, teatro, exposiciones, etc.), deportes como senderismo, piscina y fútbol, y actividades vacacionales (viajes, campamentos y excursiones). Se priorizan las actividades en entorno normalizados.

- **Respiro familiar:** se orienta a las familias de personas adultas con discapacidad. Ofrece estancias durante un fin de semana al mes para que los familiares a cargo del adulto con discapacidad puedan tener un periodo de descanso.
- **Unidad Volante de Apoyo a la Dependencia:** se dirige a personas con discapacidad o riesgo de presentarla, mayores de 26 años. Ofrece sesiones 45 minutos a domicilio, una o varias veces a la semana, de lunes a viernes. Estas sesiones pueden incluir uno o varios de los siguientes servicios: fisioterapia, logopedia, terapia ocupacional, cuidado y apoyo al dependiente, etc. Además, se ofrece atención familiar a domicilio.
- **Apoyo psicológico:** orientado a personas con discapacidad de 26 a 65 años y/o sus familiares. Ofrece, bajo cita previa, sesiones de orientación y apoyo psicológico de una hora de duración. Asimismo, ofrece servicios de diagnóstico y valoración. Su horario es de mañana o tarde.
- **Formación a familias:** ofrece cursos en horario de mañana o tarde, dirigidos a familiares de personas con discapacidad. Estos cursos tienen una duración variable y tratan sobre temas de interés para las familias (sexualidad, aspectos legales, etc.).
- **Trabajo social:** es un servicio dirigido a las familias de usuarios de servicios de APSA. Se orienta a la gestión de recursos (ayudas y becas) y solicitudes (certificado de discapacidad, reconocimiento de dependencia), atención a demandas, información y asesoramiento.
- **Actividades artísticas:** se orienta a adultos con discapacidad. Ofrece actividades de artes plásticas (cerámica, pintura) y escénicas (baile adoptado, acondicionamiento físico, nuevos ritmos), en horario de mañana y tarde.

- Vivienda: se orienta a personas con discapacidad mayores de 18 años. Ofrece alojamiento, manutención y apoyo para la vida independiente a través de diversos servicios: residencia y viviendas tuteladas.
- Programa de apoyo a la reinserción en el psiquiátrico penitenciario: se orienta a personas adultas con discapacidad que están bajo el régimen penal penitenciario en el Psiquiátrico Penitenciario de Foncalent (Alicante). Ofrece formación para el desarrollo de destrezas adaptativas y formación laboral, con el fin de favorecer la reinserción social de estas personas. Asimismo, ofrece servicios de identificación y diagnóstico, gestión de recursos, asesoría jurídica, trabajo social con el entorno del recluso, etc.

En la etapa de la Tercera Edad se ofrecen los apoyos necesarios en los últimos años de vida de la persona con discapacidad. Ofrece, entre otros, servicios de apoyo domiciliario, apoyo psicológico, ocio y deporte, etc. orientados a personas de más de 65 años.

- Programa de envejecimiento saludable: ofrece diversas actividades para favorecer el mantenimiento de la condición física y hábitos de vida saludable. Apoya a la persona con discapacidad en su envejecimiento intentando retrasar al máximo los efectos de dicho proceso. Incluye aspectos como: logopedia, fisioterapia, estimulación cognitiva, etc.
- Ocio y deporte: se orienta a personas mayores de 65 años, con discapacidad. Ofrece actividades lúdicas y de mantenimiento físico con monitores especializados como, por ejemplo: actividades recreativas, lúdicas y culturales comunitarias (cine, teatro, exposiciones, excursiones, etc.), actividades vacacionales (viajes), y actividades deportivas (mantenimiento físico, natación, etc).
- Unidad Volante de Apoyo a la Dependencia: se dirige a adultos con discapacidad, a partir de los 65 años. Ofrece sesiones de 45 minutos a domicilio, una o varias veces a la semana, de lunes a viernes. Estas sesiones pueden incluir uno a varios de los siguientes servicios: fisioterapia, logopedia, terapia ocupacional, cuidado y apoyo al

dependiente, cuidados sanitarios, etc. Además, se ofrece atención familiar a domicilio.

- Trabajo social: es un servicio dirigido a las familias de usuarios de APSA o bien personas que solicitan únicamente este servicio. Se orienta a la gestión de recursos (ayudas y becas) y solicitudes (certificado de discapacidad, reconocimiento de dependencia), atención a demandas, información y asesoramiento.
  - Apoyo psicológico: orientado a adultos con discapacidad de mayores de 65 años y/o sus familiares. Ofrece sesiones de orientación y apoyo psicológico con una duración de una hora, bajo cita previa. Asimismo, ofrece valoración continua para la actualización del certificado de discapacidad u otros reconocimientos. Su horario es de mañana o tarde.
  - Actividades artísticas: se orienta a adultos mayores de 65 años, con discapacidad. Ofrece actividades de arte plástico (cerámica, pintura) y escénico (baile adaptado, acondicionamiento físico, nuevos ritmos), en horario de mañana y tarde.
- Sedes:

En cuanto a las sedes o delegaciones con las que trabaja APSA son 10, aunque la sede Central se encuentra en Alicante (Avd. Salamanca) y se ocupa sobre todo del desarrollo infantil y la atención temprana (CDIAT). En esta sede podemos encontrar seis plantas con los servicios siguientes:

- En el sótano y planta baja vamos a encontrar el servicio de limpieza, la reprografía del sótano, el mantenimiento, los servicios generales de administración, los servicios generales, el departamento de informática y soporte, la comunicación, la psicóloga de categoría 2, fisioterapia y la dirección técnica.
- En la primera planta se encuentra la dirección del área educativa, la estimulación 3, las rss multimedia área educativa y la psicomotricidad.
- En la segunda planta se encuentra la estimulación 4, 5 y 6, así como la psicóloga de categoría 1.

- En la tercera planta se encuentra la estimulación 7, 8 y 9 y la dirección de categoría 1.
- En la cuarta planta se encuentra la estimulación 10 y 11, la Sala Snoezelen y la fisioterapia 2.
- En la quinta planta se encuentra la dirección de los proyectos de calidad, el trabajo social y la biblioteca.
- En la sexta planta se encuentra la gerencia, el departamento financiero, el departamento laboral y la dirección de sistemas TIC e infraestructuras.

Otra de las sedes se encuentra en San Vicente y se ocupa del desarrollo infantil y la atención temprana, así como es un centro de recursos y apoyo escolar (CRAE). En ella encontramos:

- La administración del centro, las Salas 1, 2, 3, 4 con la dirección del centro, 5 con la fisioterapia, las Salas del CRAE y las Salas de Fisioterapia del CRAE.

La tercera área educativa se encuentra en La Vila Joiosa y es un CDIAT y un CRAE, como la de San Vicente. Allí como salas encontramos la dirección del centro.

Después encontramos el CRAE con el Servicio de Ocio y las Actividades Artísticas en Alicante (C/Zarandietta). Allí podemos encontrar:

- En la planta baja las Salas 1, 2, 3, 4, 5, 6, 7, 8, 9 y 10, la sala polivalente 1, la sala polivalente 2 con fisioterapia y la sala polivalente 3, el servicio de ocio y la administración 1 y 2.
- En la planta 1 encontramos la dirección de la CRAE, el despacho 1 y las actividades artísticas.

En otra calle de Alicante (C/García Morato) podemos encontrar la actividad artística de Psicoballet con monitores.

En Elche podemos encontrar otra sede con un centro de formación permanente (CFP) o como APSA denomina Camí Obert y un CRAE. En esta sede podemos encontrar el Camí Obert como tal y un área educativa.

En la siguiente sede de Alicante (C/Catedrático Jaume Mas i Porcel) también podemos encontrar una sede con un CFP llamado Camí Obert. Allí podemos encontrar: la dirección del área de formación, la dirección del Camí Obert, el departamento de administración y las aulas 1, 2 y 3.

Y finalmente, podemos encontrar un CFP Camí Obert en Alfàs del Pi.

En la Partida Aguamarga de Alicante, podemos encontrar el área de empleo y el centro ocupacional Terramar. En esta sede podemos encontrar:

- Por parte del área de empleo: la dirección del área, la coordinación, las compras, el responsable de reprografía de la UMH, los responsables de reprografía de la UA, la limpieza de la UA, varios conductores y formadores profesional y un diseñador gráfico.
- Por parte del centro ocupacional Terramar: la dirección del centro ocupacional Terramar, la administración, varias psicólogas, un trabajador social, los talleres 1, 2, 3, 4, 5 y 6, el ocio y deporte, la jardinería, la cocina, la casa taller, el guarda y la casa del guarda y los autobuses 1, 2 y 3.

Finalmente, en San Juan podemos encontrar el área residencial y un centro ocupacional. Aquí podemos encontrar: la dirección del área residencial, los talleres 1, 2, 3 y 4, un trabajador social, una psicóloga del centro de día, la residencia en sí, la administración, fisioterapia, el área de salud de la residencia, el deporte y la lavandería.

A continuación, podemos encontrar un mapa con la localización de las sedes anteriormente comentadas:



<b>A</b> CFP Camí Obert Alfaz del Pi	<b>B</b> SEDE CENTRAL	<b>C</b> CRAE/ Servicio de Ocio/ Actividades Artísticas	<b>D</b> ACTIVIDADES ARTÍSTICAS	<b>E</b> CFP Camí Obert ALICANTE	<b>F</b> C.O. Terramar y ÁREA DE EMPLEO
<b>G</b> RESIDENCIA Y CENTRO OCUPACIONAL	<b>H</b> CFP CAMÍ OBERT/CRAE ELCHE	<b>I</b> SEDE REPROGRAFÍA UA	<b>J</b> CDIAT/CRAE SAN VICENTE DEL RASPEIG	<b>K</b> SEDE REPROGRAFÍA UMH	<b>L</b> CDIAT CRAE VILLAJYOYOSA

- Número de puestos de trabajo por sede o centro de trabajo:

### Salamanca

La sede está dividida en 6 plantas. También hay un sótano y una planta baja. Las plantas 5 y 6 tienen puestos de trabajo unipersonal. En el resto de plantas, se emplea 2 puestos de trabajo por despacho. En recepción existen 2 equipos, pero equivalen a 4 puestos de trabajo. En el sótano hay 2 PC más 3 servidores.

TOTAL: 61 puestos de trabajo

### La Vila

Disponen de 6 puestos de trabajo más el servidor.



TOTAL: 6 puesto de trabajo

### **Zarandieta**

Están habilitados 10 puestos de trabajos repartidos en 10 salas. También se dispone un aula con 9 puestos de trabajo incluyendo el del profesor. En los despachos, se sitúan 2 puestos de trabajo. En la zona de administración o recepción, existen 2 puestos de trabajo.

TOTAL: 25 puestos de trabajo

### **Camiobert Alicante**

En Camiobert están distribuidos 31 equipos, distribuidos entre aulas, aula de informática, área de administración y despachos. En cada aula hay 1 puesto de trabajo para el profesor, en el aula de informática hay 17 equipos y en el aula 5, hay 3 equipos para alumnos y 1 portátil para profesor.

En administración hay un equipo que funciona como 3 puestos de trabajo y una impresora.

TOTAL: 34 puestos de trabajo

### **Camiobert Elche**

Están disponibles 21 equipos para 25 puestos de trabajo.

TOTAL: 25 puestos de trabajo

### **San Vicente (CDIAT + CRAE)**

Entre ambos centros se distribuyen 10 equipos los cuales se sitúan entre las salas de tratamiento y recepción. Cada sala sirve como un único puesto de trabajo salvo el puesto de recepción que sirve como 2 puestos.

TOTAL: 10 puestos de trabajo

### **Terramar**

En la sede de Terramar disponen de 30 equipos divididos en los diferentes talleres. En la casa taller tienen diferentes despachos, algunos de ellos con 2 puestos de trabajo. En cada taller hay 2/3 equipo salvo el taller 2 que tiene un único equipo.

TOTAL: 30 puestos de trabajo

### **Residencia San Juan**

Están habilitados 25 puestos de trabajo repartidos en los diferentes despachos los cuales disponen de 1/2 puestos de trabajo. Recepción dispone de 2 equipos como 2 puestos de trabajo.

TOTAL: 25 puestos de trabajo

**Área de empleo:** En la Asociación APSA tienen un área de empleo como ya hemos visto anteriormente y uno de los servicios en los que tienen a usuarios trabajando son las reprografías situadas en la Universidad de Alicante y en la Universidad Miguel Hernández.

### **Repros UA**

Disponen de un total de 12 equipos distribuidos entre 2 locales/oficinas. Se ha habilitado una mesa con 4 equipos.

TOTAL: 12 puestos de trabajo

### **Repros UMH**

Se distribuyen diversos puestos de trabajo repartidos en 5 locales (Altea, Galia, Altabix, L'Arenal y Orihuela).

En *Altea* se dispone de 2 equipos. En *Galia*, se dispone de 3 equipos. En *Altabix*, se han habilitado 8 equipos, de los cuales el de recepción sirve como 3 puestos de trabajo. En *L'Arenal*, están habilitados 3 equipos como 3 puestos de trabajo. Y en *Orihuela*, existen 2 equipos que funcionan como 2 puestos de trabajo independientes.

TOTAL: 18 puestos de trabajo

#### **Limencop oficina**

En dicha sede, se dispone de 10 equipos que están repartidos entre talleres y despachos.

TOTAL: 10 puestos de trabajo

Disponen de 40 equipos unipersonales en el área de empleo

#### **TOTAL EQUIPOS: 222**

- Número de personas por puesto de trabajo:

#### **Salamanca**

En recepción tienen 2 equipos que sirven para 4 personas. Desde la planta bajo a la planta cuarta, cada puesto de trabajo sirve para 2 personas. En las plantas quinta y sexta, cada puesto de trabajo es unipersonal.

#### **La vila**

Cada puesto de trabajo sirve para 1/2 personas

#### **Zarandieta**

Cada puesto de trabajo es para 1 persona, salvo recepción, en la que los 2 puestos sirven para 4 personas.

#### **Camiobert Alicante**

Cada puesto de trabajo es usado por 1/2 personas. En el caso del puesto de trabajo de administración puede ser usando hasta por 4 personas.

#### **Camiobert Elche**

Cada puesto de trabajo es usado por 1/2 personas. En el caso del puesto de trabajo de administración puede ser usando hasta por 4 personas.

### **San Vicente (CDIAT + CRAE)**

Cada puesto de trabajo es unipersonal, salvo el de puesto de trabajo de recepción en el que trabajan 2 personas

### **Terramar**

Cada puesto de trabajo puede ser compartido por 2 personas

### **Residencia San Juan**

En los despachos los puestos de trabajo son unipersonales, salvo en recepción que puede ser compartido con hasta 4 personas

**Área de empleo:** En la Asociación APSA tienen un área de empleo como ya hemos visto anteriormente y uno de los servicios en los que tienen a usuarios trabajando son las reprografías situadas en la Universidad de Alicante y en la Universidad Miguel Hernández.

### **Repros UA**

Cada puesto de trabajo es compartido, depende del número de usuarios

### **Repros UMH**

Cada puesto de trabajo es compartido, depende del número de usuarios

### **Limencop**

La zona de despachos puede ser compartido cada puesto de trabajo por hasta 2 personas, mientras que en la zona de taller pueden ser varios.

**TOTAL PUESTOS DE TRABAJO: 281 puestos de trabajo aprox.**

- Otros: La Asociación APSA desarrolla una labor de atención integral a las personas con discapacidad o riesgo de padecerla de la provincia de Alicante, para ello tiene programas de prevención, atención temprana, educación, salud, formación y vivienda, y orientados a facilitar su inclusión social y laboral.

#### 4. Inventario de sistemas y usos informáticos y infraestructuras:

- La situación geográfica de los sistemas: Los sistemas se encuentran en las distintas sedes de la asociación que ya han sido mencionadas anteriormente.
- Responsables TI: Sabemos también que no hay responsables TI en cada sede pero que existe un área de TI compuesta por una Dirección y dos profesionales uno con perfil de programador-SAT y un profesional SAT para atender los sistemas TI del grupo.
- Arquitectura y configuración de hardware y software: La mayor parte de los equipos de las diferentes sedes/centros son modelos Dell que corren bajo un procesador con arquitectura Intel Core 2 duo o quad core, con 4 GB de ram de media. El sistema operativo más usado es Windows 7 seguido de Windows 10.
- Inventario de hardware y software:

Por lo que hace a los equipos hardware TI actuales del grupo APSA son los siguientes:

- 5 servidores Cloud
- 12 servidores en subredes en centros
- 47 tablets
- 222 PC's/Portátiles

Sede: Salamanca			
Situación	Procesador	Memoria	Unidades
Sótano	Intel Pentium 4	1GB	2
Planta baja	Intel Core 2 duo e7500	4GB	2
Planta 1	Intel Core 2 duo	2GB	3
Planta 2	Intel Core - Pentium	1GB – 2GB	4
Planta 3	Intel Core 2 Duo E6550	2GB	4
Planta 4	Intel Core 2 Duo E6550	2GB – 4GB	2
Planta 5	Intel (distintos tipos)	1GB – 4GB	4
Sede: La Vila			
Situación	Procesador	Memoria	Unidades
General	Intel Pentium 4	1GB	5
Sede: Zarandíeta			
Situación	Procesador	Memoria	Unidades
Planta baja	Intel (distintos tipos)	1GB – 4GB	12
Planta superior	Intel Pentium 4	1GB – 2GB	2
Sede: Camí Obert Alicante			
Situación	Procesador	Memoria	Unidades
General	Intel Pentium 4 - Celeron	1GB – 2GB	31

Sede: Camí Obert Elche			
Situación	Procesador	Memoria	Unidades
General	Intel (distintos tipos)	1GB – 2GB	21
Sede: San Vicente			
Situación	Procesador	Memoria	Unidades
CDIAT	Intel (distintos tipos)	1GB – 4GB	7
CRAE	Intel Core 2 Duo – Pentium D 820	1GB	3
Sede: Terramar			
Situación	Procesador	Memoria	Unidades
General	Intel Pentium 4 – Core 2 Duo	1GB – 4GB	30
Sede: San Juan			
Situación	Procesador	Memoria	Unidades
General	Intel y AMD	1GB – 4GB	10
Sede: Repros UA			
Situación	Procesador	Memoria	Unidades
General	Intel (distintos tipos)	1GB – 8GB	12
Sede: Repros UMH			
Situación	Procesador	Memoria	Unidades
Altea	Intel Pentium D – i3 4150	1GB – 8GB	2
Galia	AMD A10-5800K	8GB	3
Altabix	Intel y AMD	2GB – 8GB	8
L'Arenal	Intel (distintos tipos)	1GB – 8GB	3
Orihuela	Intel y AMD	8GB	2
Sede: Limencop			
Situación	Procesador	Memoria	Unidades
General	Intel Pentium 4	1 – 4GB	10
Sede: Área Empleo			
40 equipos unipersonales			

Tabla 5. Equipos APSA

(Asociación APSA)

- 105 terminales de telefonía móvil
- 29 terminales de telefonía sobremesa
- 5 instalaciones fibra óptica, 5 instalaciones ADSL
- 16 puntos de acceso inalámbrico wi-fi
- 10 proyectores
- 6 pizarras digitales
- 55 impresoras/fotocopiadoras/escáner
- 7 impresoras de tiquets
- 5 pantallas táctiles

- 185 cuentas de correo-e
  - 5 ratones adaptados
  - 5 pulsadores
- Comunicación y redes de comunicación: Referente a los sistemas de comunicación de telefonía constan de terminales móviles o sobremesa, 130, pero todos ellos con tarjetas SIM y configurados desde una centralita virtual con extensión interna corta de 4 dígitos además de la línea móvil propia. Disponen de 10 números fijos montados sobre 10 líneas móviles y de una línea de e-fax. Por otro lado, la configuración de las redes de comunicación sigue, en 5 sedes, el patrón clásico de una estructura de red por ADSL, y en las otras 5 sedes tienen fibra óptica y 2 con router con sim móvil.

La arquitectura de red de comunicación sería la siguiente:



*Ilustración 16. Arquitectura de red de comunicación*

(Asociación APSA)

- Medidas de seguridad y otros aspectos sobre problemáticas que se presentan en el área auditada: Las medidas de seguridad de software se llevan a cabo mediante el paquete de Windows Security Essentials en el caso de equipos que corran bajo Windows 7. En el caso de Windows 10 optan por Avast en su modelo de licencia gratuita.

Las copias de seguridad se realizan por medio de software (FreeFileSync) con un cifrado de seguridad media.

Los servidores, entre otros equipos, están protegidos vía hardware por un sistema SAI.

- Aplicaciones bases de datos y ficheros: En la imagen que podemos ver a continuación, podemos apreciar la arquitectura de red en la nube (cloud computing) del grupo APSA. En ella podemos ver que disponen de 5 servidores en la nube sobre los que se acceden desde las distintas sedes. En el Servidor 1 se encuentra el ERP Financiero con G2k que es un gestor para empresas G2k, facturación, contabilidad y 4 CIF's. En el Servidor 2 se encuentra la BBDD de Administración y Comunicación con Gestión de Usuarios Socios, Registro Individual de Seguimiento, Cajas Metálico, Proyectos, Demandantes de Empleo y Formación y Férulas, y también APP's Web como Gestión de tickets, Intranet documental, Reprografía virtual y Programa de Apoyo Individual. En el Servidor 3 se encuentra el ERP Laboral con SAGE 200C, RRHH y 4 CIF's. En el Servidor 4 se encuentra GSUITE y @asociacionapsa.com con usuarios ilimitados, correo-e, DRIVE, docs, hojas de cálculo, etc. Y finalmente, en el Servidor 5 se encuentran las APP's Web con la Web APSA y la Tienda Online.

Las bases de datos están todas en Sql Server Standard Edition y los tamaños de los ficheros están entre 2 y 30 GB.

Por otro lado, en cada sede disponen de servidores locales que almacenan, además de ficheros de ofimática, vídeos y fotografías y en algunas sedes tenemos entre 200GB y 3T.



## Arquitectura de Red en la nube (cloud computing) Grupo APSA

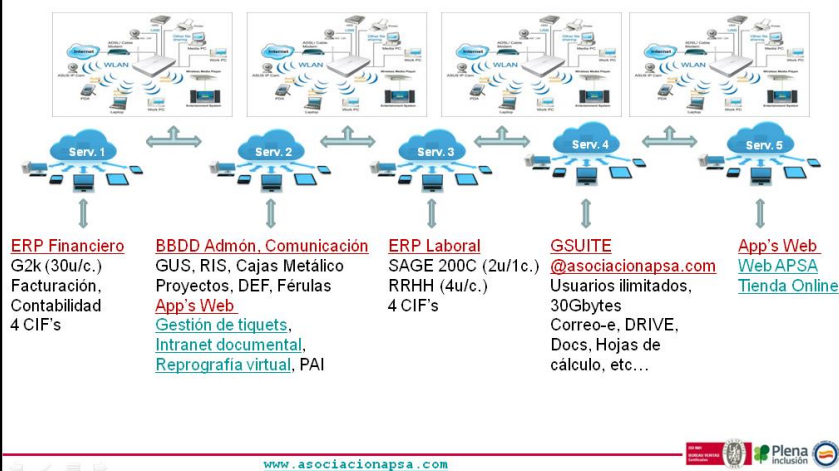


Ilustración 17. Arquitectura de Red en la nube

(Asociación APSA)

A continuación, podemos ver una lista de programas Software de Base de Datos que hay actualmente en el Grupo APSA:

- Aplicaciones corporativas (C/S y Web):
  - Gestión Usuarios Socios, GUS, RIS, DEF, ISBN
  - Gestión Cajas metálico
  - Gestión Proyectos y Contactos
  - Gestión empresarial 4 CIF's, ERP, G2k
- Aplicaciones comerciales:
  - ERP SAGE 200C
  - ERP RRHH EntiGest
- Aplicaciones Corporativas Web:
  - Gestión de tiquets
  - Intranet documental: mediante carpetas compartidas entre los usuarios del dominios
  - Tinda Online
  - Reprografía virtual
  - GSuite (Gmail, drive, docs, Excel, ppt, youtube, etc.)
  - PAI (en construcción)

- E-apsa (en construcción)

## 10.2. – Etapa de planificación

Tras el análisis, es evidente que el tamaño de la organización que se está estudiando es muy grande, por lo que para asegurar que podremos cumplir con los objetivos y plazos del TFG, consideramos interesante que la auditoría se centre en solo algunos puntos que serán los de mayor utilidad para tener una visión de cómo se encuentra la asociación.

1. Determinar los puntos que serán evaluados: Se evaluarán los puntos correspondientes al área de planificación TI ya que, así podremos averiguar como de importante es la TI para la asociación y si se planifica ésta, también se evaluarán los correspondientes a los dispositivos de almacenamiento, al funcionamiento del centro de cómputo y a la seguridad física, ya que, después de analizar la asociación y de ver cuáles son los objetivos de esta auditoría se ha creído que son las áreas en las que más se tiene que indagar.

2. Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría: Después de ver los distintos tipos de herramientas que se pueden utilizar para la auditoría, seleccionamos dos métodos distintos. Por una parte, entrevistas para extraer toda la información referente a la asociación como, por ejemplo, para saber cuál es la actividad de la asociación, cuál es su DAFO, cuáles son los pilares en los que se basa su gestión, cuáles son las sedes y delegaciones con las que trabaja la asociación, cuál es su cartera de servicios, cuál es su organigrama, cuál es el número de puestos de trabajo que hay en la asociación, cuál es la arquitectura y la configuración del hardware y del software, entre otras muchas cosas que requeríamos conocer previamente para conocer la asociación. Por otra parte, unos cuestionarios, que vamos a utilizar para realizar la auditoría TI del que hemos seleccionado preguntas correspondientes a los puntos que hemos determinado anteriormente que serán evaluados. Complementariamente, como instrumento dispondremos de la recopilación de información y la documentación que nos ha proporcionado la asociación a partir de sus propios medios.

El primer cuestionario que vamos a realizar es el correspondiente al área de planificación que se divide en las preguntas correspondientes a sistemas de información, a recursos humanos y a otros aspectos correspondientes al área de planificación, teniendo como objetivo sondear la planeación que se realizó para formar el área de sistemas, siendo de vital importancia para el desempeño del área, pues verifica si los objetivos y los alcances del área corresponden a los desempeñados. Algunas de las preguntas que podemos encontrar son [26]:

¿La dirección general y ejecutiva ha considerado la importancia que tiene el estudio del sistema de información?

¿Se recibe formación y se planifica ésta mediante asistencia a cursos, seminarios, etc.?

¿Los cambios en los sistemas informáticos son consecuencia de la planificación más que de la presión por necesidades operativas?

El segundo cuestionario que vamos a realizar es el correspondiente a los dispositivos de almacenamiento y este cuestionario tiene como objetivo evaluar la administración, la aplicación y el uso de dispositivos, hardware, de almacenamiento de información electrónico de la organización. Algunas de las preguntas que podemos encontrar son:

Los locales asignados a los servidores de datos tienen

- Aire acondicionado ( )
- Protección contra el fuego ( ) (Señalar que tipo de protección)
- Cerradura especial ( )
- Otra

¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?

En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperar los archivos?

El tercer cuestionario que vamos a realizar es el correspondiente al funcionamiento del centro de cómputo y este cuestionario tiene como objetivo evaluar el correcto funcionamiento, así como la organización del centro de cómputo, tomando en cuenta los reglamentos del área. Así como también revisar que estos reglamentos tengan como objetivo mantener el orden del centro de cómputo. Podemos encontrar preguntas como:

¿El lugar donde se ubica el centro de cómputo, está seguro de inundaciones, robo o cualquier otra situación que pueda poner en peligro los equipos?

¿La temperatura a la que trabajan los equipos es la adecuada de acuerdo a las normas bajo las cuales se rige?

¿Se cuenta con alarmas contra inundaciones?

El cuarto cuestionario que vamos a realizar es el correspondiente a la seguridad física y este cuestionario verifica la seguridad física de las instalaciones que utiliza el área de sistemas, ya que de esto depende la continuidad de los servicios que presta el área a la organización, en cuanto a necesidades de información. Y tiene preguntas del estilo siguiente:

¿Se han adoptado medidas de seguridad en el departamento de sistemas de información?

¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?

Existen extintores de fuego

a) ¿Manuales? ( )

b) ¿Automáticos? ( )

c) No existen ( )

Podemos ver todas las preguntas correspondientes a los cuatro cuestionarios en [1].

3. Elaborar planes y programas para realizar la auditoría: Para poder realizar la auditoría con éxito, vamos a empezar teniendo al menos una entrevista con posibilidad de extender a más si hiciera falta, en la que se va a recabar información sobre la asociación, estas entrevistas serán reforzadas vía email para la aclaración de pequeñas dudas, reservando así la parte presencial para las cuestiones de más peso. Estas entrevistas y este contacto, van a ser con el director TI, que es el que nos va a hacer de intermediario para resolver las distintas dudas que tengamos acerca de esta. Seguidamente, vamos a elaborar el cuestionario que hemos seleccionado como herramienta. Éste se va a enviar al director TI para que pueda ser respondido en un plazo de tiempo determinado. Una vez nos hayan respondido, vamos a determinar situación se encuentra la asociación para así definir cuáles van a tener que ser las mejoras o modificaciones para poder lograr sus objetivos, o lo que constituye redactar el *informe auditor*.

La estimación del tiempo que se va a emplear en cada una de las actividades anteriores es la siguiente: para las entrevistas estimamos que cada una de ellas va a durar entre 2 y 4 horas y que con el contacto vía email se reservará para aclarar dudas u obtener pequeños datos, lo cual no requiera emplear más de 30 minutos (tanto por el auditor como por el director TI); para la elaboración del cuestionario estimamos unas 10 horas, mientras que para que nos respondan estimamos unas 2 o 3 semanas, en las cuales además responderemos a las dudas sobre el cuestionario empleando el email; finalmente para determinar la situación en la que se encuentra estimamos 1 o 2 semana de análisis del material recopilado y para establecer las prescripciones y recomendaciones sobre la actual TI de la asociación, establecemos un plazo no inferior a 3 semanas. En cuanto a los posibles recursos que se van a emplear son: una grabadora, un PC, papel y lápiz/bolígrafo, correo electrónico y aplicaciones de ofimática (Microsoft Word, Excel y Acrobat Reader).

4. Asignar los recursos y sistemas computacionales para la auditoría: Para la realización de esta auditoría no se han utilizado recursos extra por lo que, los recursos materiales

van a ser, mail, suite ofimática, papel, lápiz y un equipo informático, en este caso un MacBook Pro y como recursos humanos, sobre todo yo, como realizadora de este TFG.

### 10.3.- Etapa de ejecución

Para empezar a conocer la Asociación realizamos una primera entrevista con el Director TI de la Asociación a finales de septiembre. En esta primera entrevista que realizamos, nos contaron a grandes rasgos como se estructuraba APSA, cuáles eran los servicios que ofertaban a sus usuarios, cuáles eran sus áreas y que edades comprendían en la atención a sus usuarios, cuáles eran las principales aplicaciones que utilizaban para la gestión general de toda la actividad (por ejemplo para la gestión de usuarios y socios), nos proporcionaron información acerca de sus infraestructuras a nivel físico y, cuáles eran sus bases de datos y como las gestionaban y nos mostraron donde están ubicados los servidores. Además de esta información, nos dieron unos documentos (varios folios) con las direcciones de las distintas sedes que forman APSA y tres folletos: el primero, llamado APSA avanzamos juntos, contenía información sobre los servicios a socios, servicios a empresas y servicios a particulares, más un poco de información sobre el grupo APSA; el segundo, llamado Cartera de Servicios APSA, contenía más información sobre APSA como cuales son los pilares de su gestión y cuál es la estructura de su cartera de servicios, así como también los servicios que ofrecen en cada etapa de su cartera de servicios; el tercero, llamado Trabaja con APSA, contenía información sobre las ventajas de trabajar con APSA y cuáles son las 10 formas de trabajar con APSA. También nos enviaron por email dos documentos Excel, uno con el inventario de los equipos de APSA y otro con el directorio del grupo APSA.

Después de esta primera reunión y de revisar el material que posteriormente se nos envió, nos hicimos una idea de lo que era la asociación APSA y nos dimos cuenta de que nos faltaba información acerca de esta, por lo que a finales de octubre tuvimos otra reunión con el Director TI. De esta segunda reunión sacamos diversos documentos, como son: el Briefing de APSA del año 2017/2018, el plan directivo TIC e Infraestructuras del 2017, y el planteamiento inicial del Proyecto e-APSA.

Como después de revisar los materiales de la última reunión nos dimos cuenta de que nos seguía faltaba información sobre la Asociación, enviamos un email pidiendo que nos informaran sobre cuál es su organigrama, cuáles son sus departamentos, cuál es el número de puestos de trabajo, cuál es el número de personas por puesto de trabajo, si hay responsables TI en cada sede, cuál es su estructura de comunicación y redes de comunicación, cuáles son las medidas de seguridad en el área informática y cuáles son las aplicaciones de bases de datos y ficheros.

Después de que nos enviaran la información de email, hicimos uso de su página web para acabar de revisar y concretar toda la información.

Ya en marzo, nos reunimos con la empresa 3dids y el director TI de APSA ya que, esta empresa es la que les ha realizado la nueva web corporativa y puesto que la web forma parte de la TI de la Asociación y la Asociación no dispone de la información de lo que están realizando, pensamos que sería de utilidad tener una reunión con ellos y que nos explicaran el desarrollo de este proyecto y así saber si nos afectaba en algo por si derivaban servicios, etc.

Después de recopilar toda esta información, como ya hemos visto en la etapa de planificación, se diseñó un cuestionario, que se acabó de diseñar en abril y se envió al director TI de APSA para que lo respondiera. Este cuestionario estaba en Word para que pudieran responder directamente en él y así facilitarles la tarea, ya que había bastantes preguntas que responder.

Nos respondieron en el plazo de tres semanas, a mitad de mayo y como al revisar las respuestas de este cuestionario vimos que había preguntas que no nos habían respondido, enviamos un email con dichas preguntas para que las respondieran, nos respondieron a los dos días y nos gustaría destacar algunas de las respuestas al cuestionario:

Por lo que hace al cuestionario correspondiente al área de planificación las respuestas que nos gustaría destacar son:

1.1 ¿La dirección general y ejecutiva ha considerado la importancia que tiene el estudio del sistema de información? SI ( ) NO ( x )

2.1 ¿Se estudia la evolución del mercado y la adaptación del personal a esa evolución? SI ( ) NO ( x )

3.1 ¿Los cambios en los sistemas informáticos son consecuencia de la planificación más que de la presión por necesidades operativas? SI ( ) NO ( x )

3.7 ¿Cuál es la inversión requerida en servicios, desarrollo y consulta a los usuarios? 95% jornada

Por lo que hace al cuestionario correspondiente a los dispositivos de almacenamiento las respuestas que nos gustaría destacar son:

4. ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos? SI ( ) NO ( x )

20. ¿Se lleva control sobre los archivos prestados por la instalación? SI ( ) NO ( x )

25. En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperar los archivos? SI ( ) NO ( x )

29. ¿Existe un procedimiento para el manejo de la información del cuarto frío? SI ( ) NO ( x )

Por lo que hace al cuestionario correspondiente al funcionamiento del centro de cómputo las respuestas que nos gustaría destacar son:

5. ¿Existe lugar suficiente para los equipos? SI ( ) NO ( x )

3. ¿El material con que está construido el centro de cómputo es confiable? SI ( ) NO ( x )



10. ¿La temperatura a la que trabajan los equipos es la adecuada de acuerdo a las normas bajo las cuales se rige? SI ( ) NO ( x )

11. ¿Se dispone de aire acondicionado? SI ( ) NO ( x )

18. ¿Los equipos cuentan con un regulador? SI ( ) NO ( x )

19. ¿Se cuenta con equipo interrumpible? SI ( ) NO ( x )

20. ¿Se tiene switch de apagado en caso de emergencia en algún lugar visible?  
SI ( ) NO ( x )

28. ¿Hay algún tipo de control de entradas y salidas de usuario? SI ( ) NO ( x )

Por lo que hace al cuestionario correspondiente a la seguridad física las respuestas que nos gustaría destacar son:

1. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información? SI ( ) NO ( x )

2. ¿Existen una persona responsable de la seguridad? SI ( ) NO ( x )

3. ¿Existe personal de vigilancia en la institución? SI ( ) NO ( x )

7. ¿Se controla el trabajo fuera de horario? SI ( ) NO ( x )

8. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas? SI ( ) NO ( x )

16. ¿Son controladas las visitas y demostraciones en el centro de cómputo?  
SI ( ) NO ( x )

17. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática? SI ( ) NO (x )

Además, se han intercambiado cerca de sesenta emails con el director TI de la Asociación APSA para aclarar dudas.

Conociendo como conocemos la empresa y conociendo hacia donde quieren ir, vamos a utilizar un marco formal para entender donde se deberían centrar los procesos de Gestión y Gobierno de TI principales en la Asociación. Después de analizar los distintos marcos y frameworks que se recogieron en el capítulo 4, hemos decidido utilizar la herramienta Cascada de Metas de COBIT ya que ésta, a partir de los objetivos de la asociación mediante las necesidades de las partes interesadas, te lleva a saber cuáles son los procesos que se deberían implantar en la organización, junto con las prácticas y las actividades para implantarlos y así lograr los objetivos relacionados con TI de una forma eficiente y efectiva maximizando la obtención de valor para las partes.

Sabemos que las necesidades de las partes interesadas son los objetivos de la Asociación, que son tanto mantener sus actuales servicios TI como incorporar los nuevos servicios TI derivados del proyecto de la Cátedra de Inclusión.

Una vez sabemos cuáles son las necesidades de las Partes Interesadas vamos a ir a Ilustración 24. Mapeo entre las Metas Corporativas y las Preguntas del Gobierno y la Gestión para analizar cuáles son las necesidades de las partes interesadas y metas empresariales, para ello vamos a responder a las preguntas siguientes de dicha ilustración.

Vamos a ponderar con un 1 las metas que consideremos que afectan a cada pregunta de manera principal y con 0.5 las que afectan de manera secundaria.

- ¿Cómo se consigue valor mediante el uso de TI? ¿Está el usuario final satisfecho con la calidad del servicio de TI?

Se consigue valor mediante el uso de TI disponiendo de una página web corporativa donde se puede encontrar información sobre la empresa, además con los nuevos

proyectos que tienen se incrementa este valor. El usuario sí que está satisfecho con la calidad del servicio TI puesto que va a disponer de gran información que le va a servir de ayuda sin tener que moverse de casa. Hemos podido observar que esta pregunta se relaciona con las metas:

- 1. Valor para los interesados de las Inversiones de Negocio. 1
- 2. Cartera de productos y servicios competitivos. 1
- 6. Cultura de servicio orientada al cliente. 1
- 7. Continuidad y disponibilidad del servicio del negocio. 1
- 13. Productividad operacional y de los empleados. 0,5
- 16. Personas preparadas y motivadas. 0,5
- 17. Cultura de innovación de producto y de negocio. 1

- ¿Cómo se gestiona el rendimiento de TI?

El rendimiento de la TI se gestiona mediante el director de la TI puesto que es el encargado de ir solucionando los problemas que surgen en ésta. Se relaciona con las metas:

- 2. Cartera de productos y servicios competitivos, de manera principal. 1
- 5. Transparencia financiera, de manera secundaria. 0,5
- 9. Toma estratégica de decisiones basada en información, de manera secundaria. 1
- 10. Optimización de los costes de los procesos del negocio. 1
- 11. Optimización de la funcionalidad de los procesos de negocio. 0,5
- 12. Programas gestionados de cambio en el negocio, de manera primaria. 1
- 14. Cumplimiento con las políticas internas. 0.5

- ¿Cómo se puede explotar mejor la tecnología de red para conseguir nuevas oportunidades estratégicas?

En estos momentos todos los servicios que la asociación presta hacia sus usuarios, son completamente presenciales. En un mundo donde tanto la educación, la asistencia e incluso el acompañamiento tiene ya un fuerte desarrollo digital, es necesario migrar al menos parte de estos servicios prestados por APSA hacia la nube, por lo que la red se comportará ahora como una infraestructura clave, al mismo nivel

que lo son las sedes en este momento. Se relaciona con las metas:

- 1. Valor para los interesados de las Inversiones de Negocio. 1
  - 2. Cartera de productos y servicios competitivos. 1
  - 8. Respuestas ágiles a un entorno de negocio cambiante. 1
  - 13. Productividad operacional y de los empleados. 0,5
  - 16. Personas preparadas y motivadas. 0,5
  - 17. Cultura de innovación de producto y de negocio. 1
- ¿Cómo puedo construir y estructurar mejor mi departamento de TI?

Como uno de los objetivos va a ser seguir manteniendo nuestros servicios y otro es incorporar los nuevos servicios, se puede estructurar mejor el departamento TI de varias maneras, como por ejemplo teniendo un encargado de la TI en cada sede. Las metas con las que lo vamos a relacionar son:

- 8. Respuestas ágiles a un entorno de negocio cambiante. 1
  - 10. Optimización de los costes de los procesos del negocio. 0,5
  - 11. Optimización de la funcionalidad de los procesos de negocio. 1
  - 12. Programas gestionados de cambio en el negocio. 1
  - 14. Cumplimiento con las políticas internas. 0,5
  - 15. Cumplimiento con políticas internas. 0,5
  - 16. Personas preparadas y motivadas. 0,5
- ¿Cuánto dependo de mis proveedores externos? ¿Cómo de bien están siendo gestionados los acuerdos de externalización de TI? ¿Cómo puedo verificarlos sobre proveedores externos?

Dependo bastante de mis proveedores externos ya que nuestros servidores están externalizados y esto podría suponer un problema serio si dejaran de funcionar.

Las metas con las que lo vamos a relacionar son:

- 3. Riesgos de negocio gestionados (salvaguarda de activos). 1
  - 4. Cumplimiento de leyes y regulaciones externas. 0,5
  - 10. Optimización de los costes de los procesos del negocio. 1
- ¿Cuáles son los requisitos (de control) para la información?

Los requisitos de control para la información son mantener un registro de quien accede a las instalaciones TI y quién accede a las bases de datos para poder cumplir el objetivo de mantener sus servicios actuales. Las metas con las que lo vamos a relacionar son:

- 4. Cumplimiento de leyes y regulaciones externas. 0,5
- 9. Toma estratégica de decisiones basada en información. 1
- 15. Cumplimiento con políticas internas, de manera secundaria. 0,5

- ¿He contemplado todos los riesgos relacionados con TI?

Se han intentado contemplar todos los riesgos relacionados con la TI ya que para que puedan seguir funcionando los servicios actuales y se puedan implantar los nuevos, deben estar contemplados y estudiados. Las metas con las que lo vamos a relacionar son:

- 3. Riesgos de negocio gestionados (salvaguarda de activos). 1
- 7. Continuidad y disponibilidad del servicio de negocio. 1
- 9. Toma estratégica de decisiones basada en información. 1
- 15. Cumplimiento con políticas internas. 0,5

- ¿Estoy ejecutando una operación de TI eficiente y robusta?

Sí que estamos ejecutando una operación de TI eficiente y robusta, sobretodo robusta puesto que es seguir con lo que tenemos y ampliar servicios. Las metas con las que lo vamos a relacionar son:

- 5. Transparencia financiera, de manera secundaria. 0,5
- 7. Continuidad y disponibilidad del servicio del negocio, de manera principal. 1

- ¿Cómo se controla el coste de TI? ¿Cómo se usan los recursos de TI en la manera más efectiva y eficiente? ¿Cuáles son las opciones de aprovisionamiento más efectivas y eficientes?

No disponemos de información sobre cómo se controla el coste de TI por lo que tampoco podemos saber cómo se usan los recursos de TI en la manera más efectiva y eficiente ya que no sabemos cuándo recursos tenemos. Así como tampoco tenemos información sobre cuáles son las opciones de aprovisionamiento más efectivas y eficientes.

- ¿Tengo suficiente personal para TI? ¿Cómo puedo desarrollar y mantener sus habilidades y cómo gestiono su rendimiento?

No disponemos de suficiente personal para TI puesto que solo hay un Director TI y dos profesionales uno con perfil de programador-SAT y un profesional SAT para atender los sistemas TI del grupo, que no dan abasto con todas las sedes. Para desarrollar sus habilidades se pueden hacer cursos para desarrollar las habilidades que se precisen y para gestionar su rendimiento se podría emplear a más personal TI, pero los recursos económicos no lo permiten.

- 10. Optimización de los costes de los procesos del negocio. 0,5
- 12. Programas gestionados de cambio en el negocio. 1
- 14. Cumplimiento con las políticas internas. 0.5

- ¿Cómo consigo confianza sobre TI?

Consigo confianza sobre TI demostrando que la TI es una parte importante para mantener los servicios que tenemos y que será necesario para que los nuevos servicios que se quieren implantar funcionen. Las metas con las que se relaciona son:

- 4. Cumplimiento de leyes y regulaciones externas. 0,5
- 15. Cumplimiento con políticas internas. 0,5

- ¿Está bien securizada la información que se está procesando?

No podemos saber si la información que se está procesando está bien securizada por lo que no podemos responder a esta pregunta con lo que no lo vamos a relacionar con ninguna meta.

- ¿Cómo se puede mejorar la capacidad de respuesta del negocio mediante un entorno de TI más flexible?

Se puede mejorar la capacidad de respuesta del negocio mediante un entorno de TI más flexible ya que se van a poder implantar mejor los nuevos servicios y se van a poder mantener los actuales. Las metas con las que se relaciona son:

- 1. Valor para los interesados de las Inversiones de Negocio. 1
- 8. Respuestas ágiles a un entorno de negocio cambiante. 1
- 16. Personas preparadas y motivadas. 0,5
- 17. Cultura de innovación de producto y de negocio. 1

- ¿Fracasan los proyectos de TI en proporcionar lo que habían prometido? Si es así, ¿por qué permanece la TI en el camino de ejecutar la estrategia de negocio?

No tenemos la suficiente información respecto a si los proyectos de TI fracasar en proporcionar lo que habían prometido ya que es el primer proyecto de TI del que tenemos conocimiento por lo que no podemos responder a esta pregunta.

- ¿Cómo es de crítica la TI para la sostenibilidad de la empresa? ¿Qué pasaría si la TI no estuviera disponible?

La TI es bastante crítica para la sostenibilidad de la empresa puesto que de ella dependen diversos servicios de nuestro negocio, aunque si la TI no estuviera disponible podríamos seguir ofreciendo algunos de los servicios tradicionales que ofrecemos.

- 1. Valor para los interesados de las Inversiones de Negocio. 1
- 2. Cartera de productos y servicios competitivos. 1
- 7. Continuidad y disponibilidad del servicio del negocio. 0,5

- ¿Qué procesos de negocio críticos dependen de TI y cuáles son los requerimientos de los procesos de negocio?

Esta pregunta no la podemos responder porque no sabemos cuáles son los procesos de negocio críticos y más aún cuáles de ellos dependen de TI y cuáles son los requerimientos de los procesos de negocio. Por ello esta pregunta no se relaciona con ninguna meta.

- ¿En cuánto han excedido de media los presupuestos de operación de TI? ¿Con qué frecuencia y cuánto se salen del presupuesto los proyectos de TI?

No podemos responder a esta pregunta porque no sabemos que parte de los presupuestos se destinan a TI y tampoco sabemos el presupuesto que habría para nuestro proyecto por lo que no podemos saber si se saldría del presupuesto. Como tampoco podemos saber con qué frecuencia y cuánto se salen del presupuesto los proyectos de TI.

- ¿Qué parte del esfuerzo de TI se dedica a apagar fuegos en lugar de facilitar las mejoras del negocio?

En nuestro proyecto hay una gran parte del esfuerzo de TI que se dedica a apagar

fuegos en lugar de facilitar las mejoras del negocio porque no hay recursos suficientes para que no sea así. Por lo que las metas que se relacionan son:

- 2. Cartera de productos y servicios competitivos. 1
- 3. Riesgos de negocio gestionados (salvaguarda de activos). 0,5
- 12. Programas gestionados de cambio en el negocio. 1

- ¿Son suficientes los recursos y la infraestructura de TI disponibles para conseguir los objetivos estratégicos de empresa requeridos?

Los recursos y la infraestructura de TI disponibles no son suficientes para conseguir los objetivos ya que como se quiere implantar nuevos servicios por lo que van a hacer falta nuevos recursos e infraestructuras. Por ello las metas con las que se relaciona son:

- 2. Cartera de productos y servicios competitivos. 1
- 5. Transparencia financiera. 0,5
- 10. Optimización de los costes de los procesos de negocio. 1
- 12. Programas gestionados de cambio en el negocio. 1

- ¿Cuánto se tarda en la toma de decisiones importantes de TI?

No disponemos de esta información por lo que no podemos responder a esta pregunta y por ello no habrá ninguna meta.

- ¿Son transparentes el esfuerzo y las inversiones totales en TI?

No disponemos de esta información por lo que no podemos responder esta pregunta y por tanto no se va a relacionar con ninguna meta.

- ¿Respalda TI a la empresa en el cumplimiento de la normativa y los niveles de servicio? ¿Cómo puedo saber si se cumple con todas las normas aplicables?

TI sí que respalda a la empresa en el cumplimiento de la normativa y los niveles de servicio porque TI es un importante respaldo en general ya que sin TI tendríamos muchos problemas actualmente por lo que suponemos que cumple la normativa y los niveles de servicio. Podemos saber si se cumple con todas las normas aplicables mediante un control.

- 4. Cumplimiento de leyes y regulaciones externas, de manera secundaria. 0,5
- 15. Cumplimiento con políticas internas, de manera secundaria. 0,5



Después de responder a todas las preguntas anteriores vamos a ver que puntuación tiene cada meta para coger las que más puntuación tengan:

1. Valor para los interesados de las Inversiones de Negocio: 4
2. Cartera de productos y servicios competitivos: 6
3. Riesgos de negocio gestionados (salvaguarda de activos): 2,5
4. Cumplimiento de leyes y regulaciones externas: 2
5. Transparencia financiera: 1,5
6. Cultura de servicio orientada al cliente: 1
7. Continuidad y disponibilidad del servicio del negocio: 3,5
8. Respuestas ágiles a un entorno de negocio cambiante: 3
9. Toma estratégica de decisiones basada en información: 3
10. Optimización de los costes de los procesos de negocio: 4
11. Optimización de la funcionalidad de los procesos de negocio: 1,5
12. Programas gestionados de cambio en el negocio: 5
13. Productividad operacional y de los empleados: 1
14. Cumplimiento con las políticas internas: 1,5
15. Cumplimiento con políticas internas: 2,5
16. Personas preparadas y motivadas: 2
17. Cultura de innovación de producto y negocio: 3

Como podemos observar hay cuatro metas que tienen mayor puntuación que el resto por lo que las metas que más relación tienen con nuestro proyecto son:

1. Valor para los interesados de las Inversiones de Negocio
2. Cartera de productos y servicios competitivos
10. Optimización de los costes de los procesos de negocio
12. Programas gestionados de cambio en el negocio

Una vez sabemos cuáles son las cuatro Metas Corporativas que más puntuación han obtenido, vamos a ir a Ilustración 25. Mapeo entre las Metas Corporativas y Metas TI para analizar cuáles son las Metas Relacionadas con TI que se relacionan con las Metas Corporativas.

Para ello vamos a ver con que Metas Relacionadas con TI se relacionan nuestras Metas Corporativas y nos quedaremos con aquellas que mayor número de principales y secundarias tengan.

	1. Valor para las partes interesadas de las Inversiones de Negocio	2. Cartera de productos y servicios competitivos	10. Optimización de los costes de los procesos de negocio	12. Programas gestionados de cambio en el negocio	Total
01 Alineamiento de TI y la estrategia de negocio	P	P	S	P	3 P 1 S
02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas					
03 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S		P	2 P 1 S
04 Riesgos de negocio relacionados con las TI gestionados				S	1 S
05 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P	P	P		3 P
06 Transparencia de los costes, beneficios y riesgos de las TI	S		P		1 P 1 S
07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S	2 P 2 S
08 Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S		3 S
09 Agilidad de las TI	S	P		S	1 P 2 S
10 Seguridad de la información, infraestructuras de procesamiento y aplicaciones					
11 Optimización de activos, recursos y capacidades de las TI	P	S	P	S	2 P 2 S

<b>12 Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio</b>	S	P	S	S	1 P 3 S
<b>13 Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad</b>	P	S	S	P	2 P 2 S
<b>14 Disponibilidad de información útil y relevante para la toma de decisiones</b>	S	S			2 S
<b>15 Cumplimiento de TI con las políticas internas</b>					
<b>16 Personal del negocio y de las TI competente y motivado</b>	S	S			2 S
<b>17 Conocimiento, experiencia e iniciativas para la innovación de negocio</b>	S	P		S	1 P 2 S

*Tabla 6. Mapeo entre Metas Corporativas y Metas TI*

Las Metas Relacionadas con TI que más principales tienen y en igualdad de principales, más secundarias son las siguientes:

- 01 Alineamiento de TI y la estrategia de negocio
- 05 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI
- 07 Entrega de servicios de TI de acuerdo a los requisitos del negocio
- 11 Optimización de activos, recursos y capacidades de las TI
- 13 Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad

Una vez sabemos cuáles son las cinco Metas Relacionadas con TI que mayor puntuación han obtenido, vamos a ir a Ilustración 26. Mapeo entre las Metas Relacionadas con la TI y los Procesos para analizar cuáles son los procesos que se relacionan con las Metas Relacionadas con la TI.

Para ello vamos a ver con que Procesos se relacionan nuestras Metas Relacionadas con TI y nos quedaremos con aquellas que mayor número de principales y secundarias tengan.

	<b>01 Alineamiento de TI y la estrategia de negocio</b>	<b>05 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI</b>	<b>07 Entrega de servicios de TI de acuerdo a los requisitos del negocio</b>	<b>11 Optimización de activos, recursos y capacidades de las TI</b>	<b>13 Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad</b>	<b>Total</b>
EDM01 - Asegurar el Establecimiento y Mantenimiento del Marco	P	S	P	S	S	2 P 3 S
EDM02 - Asegurar la Entrega de Beneficios	P	P	P	S	S	3 P 2 S
EDM03 - Asegurar la Optimización del Riesgo	S		S		S	3 S
EDM04 - Asegurar la Optimización de los Recursos	S	S	S	P	S	1 P 4 S
EDM05 - Asegurar la Transparencia hacia las partes interesadas	S		P		S	1 P 2 S
APO01 – Gestionar el marco de gestión de TI	P		S	P	S	2 P 2 S
APO02 – Gestionar la estrategia	P	S	P	S	S	2 P 3 S
APO03 – Gestionar la Arquitectura	P	S	S	P		2 P 2 S
APO04 – Gestionar la Innovación	S	P		P		2 P 1 S
APO05 – Gestionar el portafolio	P	P	S	S	P	3 P 2 S
APO06 – Gestionar el presupuesto y los costes	S	P	S	S	S	1 P 4 S

APO07 – Gestionar los Recursos Humanos	P		S	P	P	3 P 1 S
APO08 – Gestionar las Relaciones	P	S	P	S	S	2 P 3 S
APO09 – Gestionar los Acuerdos de	S	S	P	S	S	1 P 4 S
APO10 – Gestionar los Proveedores		S	P	S	S	1 P 3 S
APO11 – Gestionar la Calidad	S	P	P	S	P	3 P 2 S
APO12 – Gestionar el Riesgo			S		P	1 P 1 S
APO13 – Gestionar la Seguridad			S			1 S
BAI01 – Gestionar los Programas y Proyectos	P	P	S	S	P	3 P 2 S
BAI02 – Gestionar la Definición de Requisitos	P	S	P	S	S	2 P 3 S
BAI03 – Gestionar la Identificación y la Construcción de Soluciones	S	S	P	S	S	1 P 4 S
BAI04 – Gestionar la Disponibilidad y la Capacidad		S	P	P	S	2 P 2 S
BAI05 – Gestionar la introducción de Cambios Organizativos	S	S	S	S	P	1 P 4 S
BAI06 – Gestionar los Cambios		S	P	S	S	1 P 3 S
BAI07 – Gestionar la Aceptación del Cambio y de la Transición		S	S		S	3 S
BAI08 – Gestionar el Conocimiento	S	S	S	S		4 S
BAI09 – Gestionar los Activos			S	P		1 P 1 S
BAI10 – Gestionar la Configuración				P		1 P
DSS01 – Gestionar las Operaciones		S	P	P		2 P 1 S

DSS02 – Gestionar las Peticiones y los Incidentes del Servicio			P			1 P
DSS03 – Gestionar los Problemas		S	P	P		2 P 1 S
DSS04 – Gestionar la Continuidad	S	S	P	S		1 P 3 S
DSS05 – Gestionar los Servicios de Seguridad	S		S	S		3 S
DSS06 – Gestionar los Controles de los Procesos de Negocio			P	S		1 P 1 S
MEA01 – Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S	S	P	P	S	2 P 3 S
MEA02 – Supervisar, Evaluar y Valorar el Sistema de Control Interno			S			1 S
MEA03 – Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		S	S			2 S

*Tabla 7. Mapeo entre Metas Relacionadas con TI y Procesos*

Los procesos que más principales tienen son las siguientes:

EDM02 - Asegurar la Entrega de Beneficios

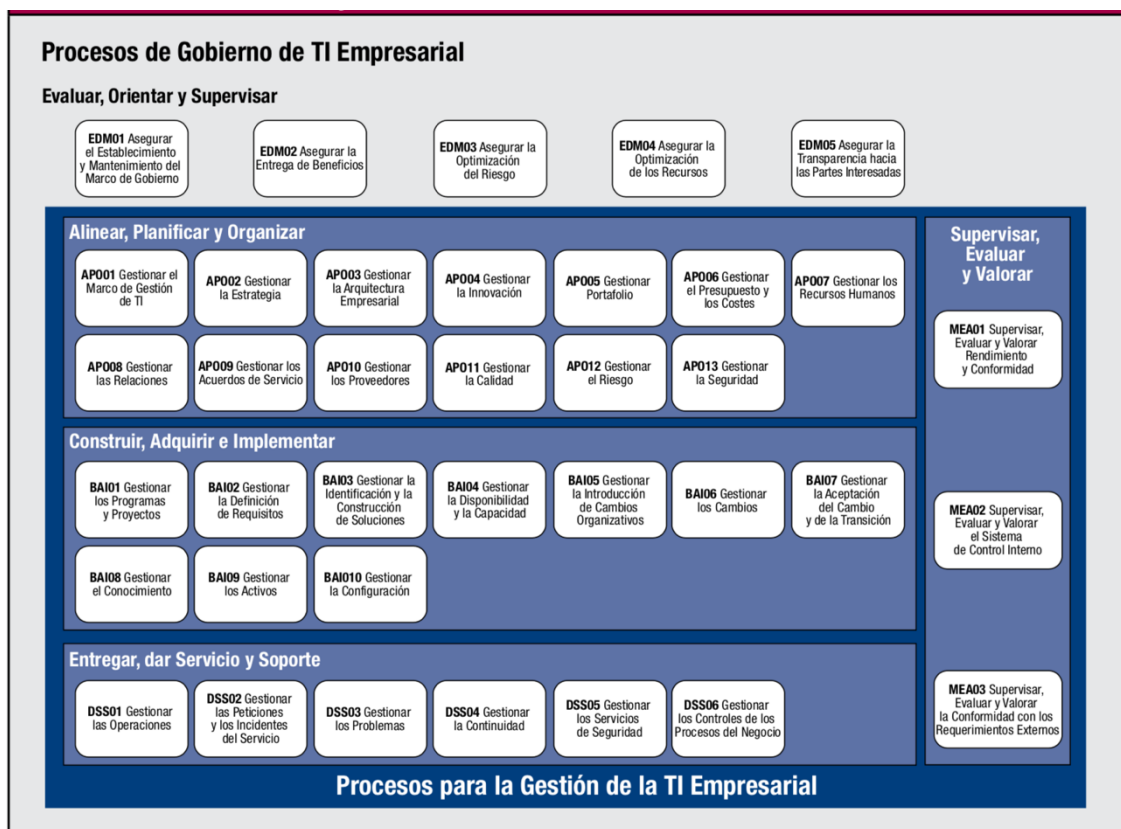
APO05 – Gestionar el portafolio

APO07 – Gestionar los Recursos Humanos

APO11 – Gestionar la Calidad

BAI01 – Gestionar los Programas y Proyectos

Ahora que ya sabemos cuáles son los procesos que debería tener APSA para cumplir sus objetivos, vamos a ver a que corresponden:



*Ilustración 18. Procesos de TI Empresarial*

Como podemos observar en la ilustración anterior, el proceso EDM02 - Asegurar la Entrega de Beneficios es un proceso de Gobierno de TI correspondiente a Evaluar, Orientar y Supervisar; los procesos APO05 – Gestionar el portafolio, APO07 – Gestionar los Recursos Humanos, APO11 – Gestionar la Calidad son procesos de Gestión de TI correspondientes a Alinear, Planificar y Organizar; y el proceso BAI01 – Gestionar los Programas y Proyectos es un proceso de Gestión de TI correspondiente a Construir, Adquirir e Implementar.

El que hayan aparecido estos 5 procesos que están relacionados tanto con el área de gobierno, como con los bloques APO y BAI del área de gestión, son coherentes dado que la asociación en estos momentos está inmersa en un profundo cambio, donde lo primero es plantear nuevos servicios, asegurar que están alineados con la asociación y su modelo de negocio e igualmente asegurar que se desarrollan. Tiene sentido que en fases posteriores otros procesos relacionados con la entrega de servicio (que ahora están en desarrollo) y la supervisión aparezcan.

## 10.4.- Etapa de dictamen

Después de realizar la auditoría en la cual hemos determinado el estado actual de la Asociación APSA, hemos podido concluir que son cinco los procesos que la asociación debería implementar para lograr alcanzar sus objetivos que, para que queden presentes cuáles son, recordamos a continuación: los objetivos de APSA son tanto mantener sus actuales servicios TI como incorporar los nuevos servicios TI derivados del proyecto de la Cátedra de Inclusión.

### 10.4.1. Proceso Asegurar la Entrega de Beneficios

El primer proceso que debería tener APSA es **Asegurar la Entrega de Beneficios**. Este proceso pertenece al área de Gobierno TI y está dentro del dominio Evaluar, Orientar y Supervisar. Este proceso sirve para optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables. Su propósito es asegurar un valor óptimo de las iniciativas de TI, servicios y activos disponibles; una entrega coste eficiente de los servicios y soluciones y una visión confiable y precisa de los costes y de los beneficios probables de manera que las necesidades del negocio sean soportadas efectiva y eficientemente.

Este proceso se divide en tres prácticas que se deberían de realizar:

- La primera de las prácticas es Evaluar la optimización de valor, es decir, evaluar continuamente las inversiones, servicios y activos del portafolio de TI para determinar la probabilidad de alcanzar los objetivos de la empresa y aportar valor a un coste razonable; identificar y juzgar cualquier cambio en la dirección que necesita ser dada a la gestión para optimizar la creación de valor.

Las actividades que se deben realizar son:

1. Comprender los requerimientos de las partes interesadas; temas estratégicos de TI, tales como la dependencia de las TI; y comprender la tecnología y sus capacidades considerando la importancia actual y potencial de TI para la estrategia de la empresa.



2. Comprender los elementos clave de gobierno necesarios para la entrega fiable, segura y coste efectiva de un valor óptimo por el uso de los servicios, activos y recursos de TI existentes y potenciales.
  3. Comprender y discutir regularmente las oportunidades que podrían surgir de los cambios habilitados en la empresa por las tecnologías actuales, nuevas o emergentes y optimizar el valor creado por estas oportunidades.
  4. Comprender lo que se entiende por valor en la empresa y considerar cómo de bien se ha comunicado, comprendido y aplicado a través de los procesos de la empresa.
  5. Evaluar la efectividad de la integración y alineamiento de las estrategias de TI en la empresa y con los objetivos de la empresa para aportar valor.
  6. Comprender y considerar cómo de efectivos son los roles, responsabilidades, asignaciones y organismos de toma de decisiones actuales asegurando la creación de valor de las inversiones, servicios y activos de TI.
  7. Considerar cómo de bien alineada está la gestión de la inversiones, servicios y activos de TI con la gestión de valor y las prácticas de gestión financiera.
  8. Evaluar la alineación del portafolio de inversiones, servicios y activos con los objetivos estratégicos de la empresa; con el valor de la empresa financiero y no financiero; con el riesgo, tanto de servicio como al del beneficio; con los procesos de negocio; la efectividad en términos de usabilidad, disponibilidad y responsabilidad; y eficiencia en términos de coste, redundancia y salud técnica.
- La segunda de las prácticas es Orientar la optimización del valor, es decir, orientar los principios y las prácticas de gestión de valor para posibilitar la realización del valor óptimo de las inversiones TI a lo largo de todo su ciclo de vida económico.

Las actividades que se deben realizar son:

1. Definir y comunicar la cartera y los tipos de inversión, categorías, criterios y ponderaciones relativas a los criterios que permitan puntuaciones de valores relativos.

2. Definir los requerimientos para los cambios de fase (stage-gate) y otras revisiones por la importancia de la inversión para la empresa y el riesgo asociado, cronograma del programa, planes de financiación y la entrega de capacidades clave y beneficios y la contribución continuada al valor.
3. Orientar a la dirección para considerar usos potenciales de TI innovadoras que posibiliten que la empresa responda a nuevas oportunidades y desafíos, lleve a cabo nuevos negocios, incremente la competitividad o mejore sus procesos.
4. Orientar los cambios necesarios en la asignación de imputaciones y responsabilidades en la ejecución del portafolio de inversiones y la entrega de valor a partir de los servicios y procesos de negocio.
5. Definir y comunicar a nivel de empresa los objetivos de entrega de valor y las medidas de resultados para permitir un control eficaz.
6. Orientar los cambios necesarios en la cartera de inversiones y servicios para realinearlos con los objetivos de la empresa actuales y esperados y/o sus limitaciones.
7. Recomendar la consideración de innovaciones potenciales, cambios organizativos o mejoras operativas que desde las iniciativas TI pudieran impulsar un incremento de valor para la empresa.

- La tercera de las prácticas es Supervisar la optimización de valor, es decir, supervisar los indicadores clave y sus métricas para determinar el grado en que el negocio está generando el valor y los beneficios previstos de los servicios e inversiones TI; identificar los problemas significativos y considerar las acciones correctivas.

Las actividades que se deben realizar son:

1. Definir un conjunto equilibrado de objetivos de desempeño, métricas, metas y puntos de referencia. Las métricas deberían cubrir la actividad y la medida de resultados, incluyendo los indicadores de retardo y de avance de los resultados, así como un equilibrio adecuado de las medidas financieras y no financieras. Revisarlos y acordarlos con las funciones de TI y de negocio, y otras partes interesadas relevantes.

2. Recoger los datos pertinentes, oportunos, completos, fiables y precisos para informar sobre los avances en la entrega de valor respecto a los objetivos. Obtener una sucinta, de alto nivel, completa vista de la cartera, programa y desempeño TI (capacidades técnicas y operativas) que soporten la toma de decisiones y aseguren que los resultados esperados se están logrando.

3. Conseguir informes habituales y relevantes de la cartera, programa y desempeño de TI (tecnológico y funcional). Revisar el progreso de la empresa hacia los objetivos identificados y el grado en el que los objetivos previstos son alcanzados, los entregables obtenidos, los objetivos de rendimiento alcanzados y el riesgo mitigado.

4. Tras la revisión de los informes, tomar las medidas de gestión apropiadas según sea necesario para asegurar que el valor sea optimizado.

5. Tras la revisión de los informes, asegúrese de que las medidas correctivas apropiadas son iniciadas y controladas.

Para la monitorización del desarrollo del proceso es necesario que se implanten y se controlen indicadores que permitan conocer el grado de éxito del proceso, y esto se llevará a cabo mediante el registro de ciertas métricas. Algunas de las métricas que se podrían utilizar para evaluar el correcto funcionamiento del proceso son:

- Porcentaje de iniciativas TI en el portafolio general en las que el valor está siendo gestionado a través del ciclo de vida completo. Esto se podría saber contando el número de iniciativas TI donde el valor es gestionado a través del ciclo de vida completo, sobre el total de iniciativas del portafolio.
- Porcentaje del valor esperado realizado. Esto se podría calcular estimando cuál es el valor final esperado y midiendo el valor final obtenido real.

Este proceso tiene sentido desde el punto de vista de que, la transformación digital que va a sufrir la asociación la va a convertir totalmente en dependiente de la TI, donde ahora igual sus servicios eran más dependientes del contacto humano, con los nuevos serán dependientes de la TI, con lo que es importante controlar y asegurar que los beneficios se están logrando y en qué medida estos beneficios emanan de la TI.

#### 10.4.2 Proceso Gestionar el Portafolio

El segundo proceso que debería tener APSA es **Gestionar el Portafolio**. Este proceso pertenece al área de Gestión TI y está dentro del dominio Alinear, Planificar y Organizar. Este proceso sirve para ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación; evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos así como en su valor y riesgo corporativo; mover los programas seleccionados al portafolio de servicios activos listos para ser ejecutados; supervisar el rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas. Su propósito es optimizar el rendimiento del portafolio global de programas en respuesta al rendimiento de programas y servicios y a las cambiantes prioridades y demandas corporativas.

Este proceso se divide en seis prácticas que se deberían de realizar:

- La primera de las prácticas es Establecer la mezcla del objetivo de inversión, es decir, revisar y garantizar la claridad de las estrategias y servicios actuales corporativos y de TI; definir una adecuada mezcla de inversión, basada en los costes, la alineación con la estrategia y medidas financieras, tales como coste, retorno de inversión esperado a lo largo de todo el ciclo de vida económico, grado de riesgo y tipo de beneficio para los programas del portafolio; ajustar las estrategias corporativas y de TI cuando sea necesario.

Las actividades que se deben realizar son:

1. Validar que las inversiones TI y los servicios TI actuales están alineados con la visión y los principios corporativos, metas y objetivos estratégicos, visión de la arquitectura empresarial y prioridades.
2. Conseguir un entendimiento común entre TI y otras funciones de negocio sobre las potenciales oportunidades de TI para conducir y sustentar la estrategia corporativa.

3. Crear una mezcla de inversión que logre el balance adecuado entre distintas dimensiones, incluyendo el equilibrio justo de retornos a corto y largo plazo, beneficios financieros y no financieros e inversiones de alto y bajo riesgo.

4. Identificar las categorías generales de sistemas de información, aplicaciones, datos, servicios de TI, infraestructura, activos de TI, recursos, habilidades, prácticas, controles y relaciones necesarias para sustentar la estrategia corporativa.

5. Acordar una estrategia TI y unas metas, considerando las interrelaciones existentes entre la estrategia corporativa y los servicios TI, activos y otros recursos. Identificar y facilitar sinergias que puedan ser alcanzadas.

- La segunda de las prácticas es Determinar la disponibilidad y las fuentes de fondos, es decir, determinar las fuentes potenciales de fondos, diferentes opciones de financiación y las implicaciones de las fuentes de financiación sobre las expectativas del retorno de inversión.

Las actividades que se deben realizar son:

1. Entender la disponibilidad y el compromiso de los fondos actuales, el gasto actual aprobado y la cantidad real gastada hasta la fecha.

2. Identificar las opciones para obtener financiación adicional para las inversiones TI internamente o de fuentes externas.

3. Determinar las implicaciones de la fuente de financiación en las expectativas de retorno de la inversión.

- La tercera de las prácticas es Evaluar y seleccionar los programas a financiar, es decir, basado en los requisitos de la mezcla general del portafolio de inversión, evaluar y priorizar casos de negocio de programas y decidir sobre las propuestas de inversión, así como también dedicar fondos e iniciar los programas.

Las actividades que se deben realizar son:

1. Reconocer las oportunidades de inversión y clasificarlas en línea con las categorías del portafolio de inversiones. Especificar los resultados empresariales esperados, todas las iniciativas necesarias para alcanzar los resultados esperados, costes, dependencias y riesgos y como todo debe ser medido.
2. Realizar evaluaciones detalladas de todos los casos de negocio de los programas, evaluando el alineamiento estratégico, beneficios corporativos, riesgo y disponibilidad de recursos.
3. Evaluar el impacto en el portafolio general de inversiones por añadir los programas candidatos, incluyendo cualquier cambio que pueda ser requerido por otros programas.
4. Decidir qué programas candidatos deberían ser trasladados al portafolio de inversiones activas. Determinar si los programas rechazados deberían ser conservados para ser considerados en el futuro, o provistos con algún tipo de inversión para determinar si el caso de negocio puede ser mejorado o descartado.
5. Determinar los hitos necesarios para el ciclo de vida económico de cada programa seleccionado. Asignar y reservar totalmente los fondos para cada hito. Mover el programa al portafolio de inversiones activas.
6. Establecer procedimientos para comunicar el coste, beneficios y aspectos relativos al riesgo de esos portafolios a los procesos de priorización de presupuesto, gestión del coste y gestión del beneficio.

- La cuarta de las prácticas es Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones, es decir, regularmente, supervisar y optimizar el rendimiento del portafolio de inversiones y de los programas individuales a lo largo de todo el ciclo de vida de inversión.

Las actividades que se deben realizar son:

1. Revisar regularmente el portafolio para identificar y explotar sinergias, eliminar programas duplicados e identificar y mitigar el riesgo.

2. Cuando sucedan cambios, volver a evaluar y a priorizar el portafolio para asegurar que está alineado con la estrategia del negocio y que la mezcla de inversión objetivo se mantiene, de modo que el portafolio esté optimizado el valor global. Esto puede requerir que los programas cambien, se aplacen, se retiren o bien que nuevos programas se inicien.

3. Ajustar los objetivos, previsiones, presupuestos y, si fuese necesario, el grado de monitorización empresariales para reflejar los gastos en que se incurriría y los beneficios de la empresa que se obtendrían gracias a los programas del portafolio de inversiones activas. Incorporar los gastos del programa en el mecanismo de prorrateo de costes.

4. Proporcionar una vista precisa a las partes interesadas sobre el rendimiento del portafolio de inversiones.

5. Aportar informes ejecutivos para la revisión por parte de la alta dirección de los progresos de la empresa hacia las metas identificadas, estableciendo qué debe seguir siendo gastado y conseguido sobre qué franjas temporales.

6. Incluir en la supervisión periódica del rendimiento información sobre en qué medida los objetivos planificados han sido alcanzados, el riesgo mitigado, las capacidades creadas, los entregables obtenidos y las metas de rendimiento, conseguidas.

7. Identificar desviaciones para:

- Control presupuestario entre el real y el presupuesto
- Gestión del beneficio de:
  - Real versus objetivos de inversión en soluciones, probablemente expresados en términos de retorno de la inversión (ROI), valor actual neto (NPV) o tasa interna de retorno (IRR)
  - Tendencia actual del coste del portafolio de servicios para la mejora de la productividad de la entrega del servicio

8. Desarrollar métricas para medir la contribución de TI a la empresa, y establecer objetivos de rendimiento adecuados que reflejen las metas de capacidad corporativas y

de TI. Utilizar asistencia de expertos y de datos de análisis comparativos para desarrollar métricas.

- La quinta de las prácticas es Mantener los portafolios, es decir, mantener los portafolios de programas y proyectos de inversión, servicios de TI y activos de TI.

Las actividades que se deben realizar son:

1. Crear y mantener portafolios de programas de inversiones TI, servicios TI y activos TI, que constituyan la base del presupuesto actual de TI y soporten los planes estratégicos y tácticos de TI.

2. Trabajar con los responsables de entrega del servicio para mantener los portafolios de servicios y con los responsables de operaciones y arquitectos para mantener el portafolio de activos. Apoyar los planes tácticos y estratégicos de TI.

3. Eliminar los programas del portafolio de inversiones activas cuando los beneficios corporativos deseados han sido alcanzados o cuando está claro que los beneficios no serán alcanzados dentro del criterio de valor establecido para el programa.

- La sexta de las prácticas es Gestionar la consecución de beneficios, es decir, supervisar los beneficios de proporcionar y mantener servicios y capacidades TI apropiadas, basadas en el caso de negocio acordado actual.

Las actividades que se deben realizar son:

1. Utilizar las métricas acordadas y realizar seguimiento sobre cómo los beneficios son obtenidos, cómo evolucionan a lo largo del ciclo de vida de programas y proyectos, cómo son entregados desde los servicios TI y cómo resultan al someterlos a un análisis comparativo interno y de la industria. Comunicar los resultados a las partes interesadas.

2. Implementar acciones correctivas cuando los beneficios alcanzados se desvían significativamente de los esperados. Actualizar los casos de negocio para las nuevas iniciativas e implementar procesos de negocio y mejoras del servicio según se requiera.



3. Considerar obtener orientación de expertos externos, líderes de la industria y datos de análisis comparativos para probar y mejorar las métricas y los objetivos.

Para la monitorización del desarrollo del proceso es necesario que se implanten y se controlen indicadores que permitan conocer el grado de éxito del proceso, y esto se llevará a cabo mediante el registro de ciertas métricas. Algunas de las métricas que se podrían utilizar para evaluar el correcto funcionamiento del proceso son:

- Grado hasta el que la dirección corporativa está satisfecha con la contribución de TI a la estrategia empresarial. Esto se podría saber realizando una encuesta anual, que se pasaría a la directiva, donde se pregunte el grado de satisfacción con la contribución de TI a la estrategia empresarial, esto es preguntar si están muy poco satisfechos, poco satisfechos, bastante satisfechos o muy satisfechos.
- Porcentaje de inversiones TI que tiene trazabilidad con la estrategia de la compañía. Esto se podría saber contando el número de inversiones TI que tienen trazabilidad con la estrategia de la Asociación con respecto de las inversiones TI totales.

Este proceso tiene sentido desde el punto de vista de que la Asociación con el objetivo de tener y prestar nuevos servicios a sus clientes, debe diseñar cuidadosamente su portfolio de servicios, ya que estos servicios se convertirán en los nuevos servicios que preste a su comunidad de socios y por lo tanto aquellos que se constituirán en la nueva fuente de ingresos. Estos servicios han de ser diseñados de forma que se asegure el retorno de la inversión, la maximización de los beneficios, la adecuación de los servicios a la estrategia y arquitectura de la empresa y a una gestión eficiente de los recursos. Por lo que ahora una de las principales tareas del área de gestión es asegurar que estos nuevos servicios digitales que van a ser prestados aseguran estas características.

#### 10.4.3 Proceso Gestionar los Recursos Humanos

El tercer proceso que debería tener APSA es **Gestionar los Recursos Humanos**. Este proceso pertenece al área de Gestión TI y está dentro del dominio Alinear, Planificar y Organizar. Este proceso sirve para proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades

de los recursos humanos; esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada. Su propósito es optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa.

Este proceso se divide en seis prácticas que se deberían de realizar:

- La primera de las prácticas es Mantener la dotación de personal suficiente y adecuada, es decir, evaluar las necesidades de personal en forma regular o en cambios importantes en la empresa, operativos o en los entornos para asegurar que la empresa tiene suficientes recursos humanos para apoyar las metas y objetivos empresariales. El personal incluye recursos tanto internos como externos.

Las actividades que se deben realizar son:

1. Evaluar las necesidades de personal de forma regular o ante cambios importantes para asegurar que:

- La función de TI cuenta con recursos suficientes para apoyar de manera adecuada y apropiada las metas y objetivos empresariales.
- La empresa cuenta con recursos suficientes para apoyar de manera adecuada y apropiada los procesos de negocio y los controles e iniciativas TI.

2. Mantener los procesos de contratación y de retención del personal de TI y del negocio en línea con las políticas y procedimientos de personal globales de la empresa.

3. Incluir controles de antecedentes en el proceso de contratación de TI para empleados, contratistas y proveedores. El alcance y la frecuencia de estos controles depende de la sensibilidad y/o criticidad de la función.

4. Establecer mecanismos flexibles de dotación de recursos para apoyar a las necesidades cambiantes del negocio, tales como el uso de transferencias, contratistas externos y acuerdos de servicio con terceras partes.

5. Asegurarse de que el entrenamiento cruzado se lleva a cabo y que hay respaldo para el personal clave para reducir la dependencia de una sola persona.

- La segunda de las prácticas es Identificar personal clave de TI, es decir, identificar el personal clave de TI a la vez que se reduce al mínimo la dependencia de una sola persona en la realización de una función crítica de trabajo mediante la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión y el respaldo (backup) de personal.

Las actividades que se deben realizar son:

1. Minimizar la dependencia en una sola persona en la realización de una función crítica de trabajo mediante la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión, el respaldo (backup) del personal, el entrenamiento cruzado e iniciativas de rotación de puestos.

2. Como medida de seguridad, proporcionar directrices sobre un tiempo mínimo de vacaciones anuales que deben tomar los individuos clave.

3. Tomar acciones expeditivas con respecto a cambios laborales, especialmente despidos.

4. Probar regularmente los planes de respaldo (backup) del personal.

- La tercera de las prácticas es Mantener las habilidades y competencias del personal, es decir, definir y gestionar las habilidades y competencias necesarias del personal. Verificar regularmente que el personal tenga las competencias necesarias para cumplir con sus funciones sobre la base de su educación, formación y/o experiencia y verificar que estas competencias se mantienen, con programas de capacitación y certificación en su caso. Proporcionar a los empleados aprendizaje permanente y oportunidades para mantener sus conocimientos, habilidades y competencias al nivel requerido para conseguir las metas empresariales.

Las actividades que se deben realizar son:

1. Definir las habilidades y competencias necesarias y disponibles actualmente tanto de recursos internos como externos para lograr los objetivos de empresa, de TI y de procesos.
  2. Proporcionar una planificación formal de la carrera y desarrollo profesional para fomentar el desarrollo de competencias, oportunidades de progreso personal y una menor dependencia de personas clave.
  3. Proporcionar acceso a repositorios de conocimiento para apoyar el desarrollo de habilidades y competencias.
  4. Identificar las diferencias entre las habilidades necesarias y las disponibles y desarrollar planes de acción para hacerles frente de manera individual y colectiva, tales como formación (técnica y en habilidades de comportamiento), contratación, redistribución y cambios en las estrategias de contratación.
  5. Desarrollar y ejecutar programas de formación basados en los requisitos organizativos y de procesos, incluidos los requisitos sobre conocimiento empresarial, control interno, conducta ética y seguridad.
  6. Llevar a cabo revisiones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos y externos. Revisar la planificación de la sucesión.
  7. Revisar los materiales y programas de formación de manera regular para asegurarse su adecuación a los requisitos empresariales cambiantes y su impacto en los conocimientos, aptitudes y habilidades necesarias.
- La cuarta de las prácticas es Evaluar el desempeño laboral de los empleados, es decir, lleve a cabo oportunamente evaluaciones de rendimiento de manera regular respecto a los objetivos individuales derivados de los objetivos de la empresa, las normas establecidas, las responsabilidades específicas del trabajo y el marco de habilidades y competencias. Los empleados deberían recibir preparación sobre el desempeño y conducta siempre que sea apropiado.

Las actividades que se deben realizar son:

1. Considerar los objetivos funcionales/de empresa como el contexto para establecer las metas individuales.
  2. Establecer los objetivos individuales alineados con los objetivos de los procesos relevantes, de modo que exista una clara contribución a los objetivos de TI y empresariales. Basar las metas en objetivos SMART (específicos, medibles, realizables, pertinentes y de duración determinada) que reflejen las competencias básicas, los valores empresariales y las habilidades necesarias para la(s) función(es).
  3. Recopilar los resultados de la evaluación de desempeño de 360 grados.
  4. Implementar y comunicar un proceso disciplinario.
  5. Proporcionar instrucciones específicas para el uso y almacenamiento de información personal en el proceso de evaluación, de conformidad con la legislación laboral y sobre datos personales aplicables.
  6. Proporcionar retroalimentación oportuna sobre el desempeño frente a las metas del individuo.
  7. Implementar un proceso de remuneración/reconocimiento que premie el compromiso adecuado, el desarrollo de competencias y el logro exitoso de los objetivos de desempeño. Asegurar que el proceso se aplica de forma coherente y en consonancia con las políticas de la organización.
  8. Desarrollar planes de mejora del desempeño basados en los resultados del proceso de evaluación y los requisitos de capacitación y desarrollo de competencias identificados.
- La quinta de las prácticas es Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio, es decir, comprender y realizar un seguimiento de la demanda actual y futura de recursos humanos para el negocio y TI con responsabilidades en TI corporativa. Identificar las carencias y proporcionar datos de entrada a los planes de aprovisionamiento, planes de abastecimiento de procesos de contratación del negocio y de TI y procesos de contratación del negocio y de TI.

Las actividades que se deben realizar son:

1. Crear y mantener un inventario de recursos humanos de negocio y TI.
2. Entender la demanda actual y futura de recursos humanos para apoyar el logro de los objetivos de TI y ofrecer servicios y soluciones basados en la cartera de las iniciativas actuales relacionadas con las TI, la cartera de inversiones futuras y las necesidades operativas del día a día.
3. Identificar las carencias y proporcionar datos de entrada a planes de aprovisionamiento, así como a los procesos de contratación de la empresa y de TI. Crear y revisar el plan de personal, haciendo seguimiento del uso real.
4. Mantener información adecuada sobre el tiempo dedicado a diferentes tareas, trabajos, servicios o proyectos.

- La sexta de las prácticas es Gestionar el personal contratado, es decir, asegurarse de que los consultores y el personal contratado que apoyan a la empresa con capacidades de TI conocen y cumplen las políticas de la organización, así como los requisitos contractuales previamente acordados.

Las actividades que se deben realizar son:

1. Implementar políticas y procedimientos que describan cuándo, cómo y qué tipo de trabajo puede ser realizado o incrementado por consultores y/o contratistas, de acuerdo con la política de contratación de TI de la organización y el marco de control de TI.
2. Obtener un acuerdo formal por parte de los contratistas en el inicio del contrato en cuanto a que están obligados a cumplir con el marco de control de TI de la empresa, tal como políticas de control de seguridad, control de acceso físico y lógico, uso de las instalaciones, requisitos de confidencialidad de la información y los acuerdos de confidencialidad.

3. Advertir a los contratistas de que la gerencia se reserva el derecho de supervisar e inspeccionar todo uso de los recursos de TI, incluyendo correo electrónico, comunicaciones de voz y todos los programas y archivos de datos.
4. Proporcionar a los contratistas una definición clara de sus funciones y responsabilidades como parte de sus contratos, incluidos requisitos explícitos para documentar su trabajo en base a normas y formatos previamente acordados.
5. Revisar el trabajo de los contratistas y basar la aprobación de los pagos en los resultados.
6. Definir todo el trabajo a realizar por terceras partes en contratos formales y sin ambigüedades.
7. Llevar a cabo revisiones periódicas para asegurarse de que el personal contratado ha firmado y aceptado todos los acuerdos necesarios.
8. Llevar a cabo revisiones periódicas para asegurarse de que las funciones de los contratistas y sus derechos de acceso son adecuados y en línea con los acuerdos.

Para la monitorización del desarrollo del proceso es necesario que se implanten y se controlen indicadores que permitan conocer el grado de éxito del proceso, y esto se llevará a cabo mediante el registro de ciertas métricas. Algunas de las métricas que se podrían utilizar para evaluar el correcto funcionamiento del proceso son:

- Número de decisiones que no pudieron resolverse dentro de las estructuras de gestión y se escalaron a las estructuras de gobierno. Esto se podría medir teniendo un seguimiento de las decisiones que no pudieron resolverse dentro de las estructuras de gestión y tuvieron que escalarse a las estructuras de gobierno ya sea mensual o anualmente.
- Porcentaje de puestos de TI vacantes. Esto se podría medir contando el número de puestos de TI vacantes sobre el total de puestos vacantes.

Este proceso tiene sentido desde el punto de vista de que, al prestar nuevos servicios TI, van a tener que gestionar sus recursos humanos tanto para poder seguir ofreciendo sus

antiguos servicios como para poder llegar a ofrecer los nuevos que se quieren implantar. La plantilla de personal hasta ahora ha contado con un desarrollo profesional y formación relacionada con los servicios prestados hasta ahora, pero en el nuevo panorama de servicios digitales es necesario que el personal se forme adecuadamente, se mantenga una relación adecuada con el personal, y la empresa se asegure de que las personas involucradas tienen los recursos suficientes para desempeñar su función.

#### 10.4.4 Proceso Gestionar la Calidad

El cuarto proceso que debería tener APSA es **Gestionar la Calidad**. Este proceso pertenece al área de Gestión TI y está dentro del dominio Alinear, Planificar y Organizar. Este proceso sirve para definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia. Su propósito es asegurar la entrega consistente de soluciones y servicios que cumplan con los requisitos de la organización y que satisfagan las necesidades de las partes interesadas.

Este proceso se divide en seis prácticas que se deberían de realizar:

- La primera de las prácticas es Establecer un sistema de gestión de la calidad (SGC), es decir, establecer y mantener un SGC que proporcione una aproximación a la gestión de la calidad para la información, la tecnología y los procesos de negocio que sea continua, estandarizada, formal y que esté alineada con los requerimientos del negocio y con la gestión de la calidad a nivel corporativo.

Las actividades que se deben realizar son:

1. Asegurar que el marco de control de TI, el negocio y los procesos de TI incluyen un enfoque estándar, formal y continua de gestión de la calidad que está alineado con los requerimientos empresariales. Dentro del marco de control de TI y de los procesos de negocio y de TI, identificar los requisitos y criterios de calidad (por ejemplo, sobre la base de los requerimientos legales y los requisitos de los clientes).



2. Definir roles, tareas, capacidades de decisión y responsabilidades para la gestión de la calidad, dentro de la estructura organizativa.
3. Definir planes de gestión de la calidad para los procesos, proyectos u objetivos importantes, que estén alineados con los criterios y políticas del sistema de la calidad a nivel corporativo. Registrar los datos relacionados con la calidad.
4. Supervisar y medir la eficacia y la aceptación de la gestión de la calidad, y mejorarla cuando sea necesario.
5. Alinear la gestión de la calidad TI con la gestión de la calidad a nivel corporativo fomentando un enfoque de la calidad estandarizado y continuo.
6. Obtener los inputs necesarios de las partes interesadas internas y externas para la definición de los requisitos y los criterios de aceptación de la calidad.
7. Comunicar de manera eficaz el enfoque (por ejemplo, mediante programas de formación en calidad formales y regulares).
8. Revisar periódicamente la relevancia, eficiencia y eficacia de los procesos específicos de gestión de calidad. Supervisar el cumplimiento de los objetivos de la calidad.

- La segunda de las prácticas es Definir y gestionar estándares, procesos y prácticas de calidad, es decir, identificar y mantener los requisitos, normas, procedimientos y prácticas de los procesos clave para orientar a la organización en el cumplimiento del SGC. Este debería estar en consonancia con los requisitos del marco de control TI. Considerar la posibilidad de certificar los procesos, las unidades de la organización, los productos o los servicios clave.

Las actividades que se deben realizar son:

1. Definir las normas, procedimientos y prácticas de gestión de la calidad en consonancia con los requisitos del marco de control TI. Hacer uso de las mejores prácticas de la industria como referencia para la mejora y adaptación de los procesos de gestión de la calidad de la empresa.

2. Considerar los costes y los beneficios de las certificaciones de calidad.

- La tercera de las prácticas es Enfocar la gestión de la calidad en los clientes, es decir, enfocar la gestión de la calidad en los clientes, mediante la determinación de sus necesidades y asegurar el alineamiento con las prácticas de gestión de calidad.

Las actividades que se deben realizar son:

1. Enfocar la gestión de la calidad en los clientes, mediante la determinación de los requisitos de los clientes externos e internos y asegurando el alineamiento de las normas y prácticas de TI. Definir y comunicar los roles y responsabilidades relativos a la resolución de conflictos entre clientes/usuarios y la organización TI.

2. Gestionar las necesidades y las expectativas del negocio para cada proceso de negocio, servicio operativo y nuevas soluciones de TI y mantener sus criterios de aceptación de la calidad. Capturar los criterios de aceptación de la calidad para su inclusión en los acuerdos de nivel de servicio (ANS).

3. Comunicar los requisitos y expectativas del cliente por toda la organización de negocio y de TI.

4. Obtener periódicamente los puntos de vista del cliente sobre los procesos de negocio y la provisión de servicios y la entrega de soluciones TI, para determinar el impacto sobre las normas y prácticas de TI y garantizar que se cumplen las expectativas de los clientes y se actúa en consecuencia.

5. Supervisar y revisar regularmente que el SGC está de acuerdo a los criterios de aceptación de la calidad. Incluir los comentarios de los clientes, usuarios y la dirección. Responder a las discrepancias en los resultados de las revisiones para lograr una mejora continua del SGC.

6. Capturar los criterios de aceptación de la calidad para su inclusión en los ANS.

- La cuarta de las prácticas es Supervisar y hacer controles y revisiones de la calidad, es decir, supervisar la calidad de los procesos y servicios de forma permanente como se defina en el SGC. Definir, planificar y aplicar medidas para supervisar la satisfacción del

cliente con la calidad, así como el valor que proporciona el SGC. La información recogida debería ser utilizada por los propietarios de los procesos para mejorar la calidad.

Las actividades que se deben realizar son:

1. Supervisar la calidad de los procesos y servicios de forma permanente y sistemática mediante la descripción, las métricas, los análisis, la mejora/ingeniería y controles de los procesos.
2. Preparar y llevar a cabo revisiones de calidad.
3. Informar de los resultados de las revisiones y poner en marcha las mejoras necesarias.
4. Supervisar la calidad de los procesos, así como el valor proporcionado por la calidad. Asegurar que la medición, supervisión y registro de la información es utilizada por los propietarios de los procesos para tomar las acciones correctivas y preventivas necesarias.
5. Supervisar las métricas de calidad basadas en objetivos alineadas con los objetivos generales de calidad y cubriendo la calidad de todos los servicios y los proyectos individuales.
6. Asegurar que la dirección y los propietarios de los procesos revisan periódicamente el rendimiento de la gestión respecto a las métricas de calidad definidas.
7. Analizar los resultados del rendimiento de la gestión de la calidad global.

- La quinta de las prácticas es Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios, es decir, incorporar las prácticas pertinentes de gestión de la calidad en la definición, supervisión, notificación y gestión continua del desarrollo de soluciones y servicios ofrecidos.

Las actividades que se deben realizar son:

1. Integrar las prácticas de gestión de la calidad en los procesos y prácticas de desarrollo de soluciones.

2. Supervisar de manera continua los niveles de servicio e incorporar prácticas de gestión de la calidad en todos los procesos y prácticas de prestación de servicios.

3. Identificar y documentar las causas raíz de las no conformidades y comunicar los resultados a la dirección de TI y otras partes interesadas de manera oportuna para permitir que se adopten las medidas correctivas oportunas. Cuando sea necesario, realizar el seguimiento de las revisiones.

- La sexta de las prácticas es Mantener una mejora continua, es decir, mantener y comunicar regularmente un plan de la calidad global que promueva la mejora continua. Esto debería incluir la necesidad y los beneficios de una mejora continua. Recoger y analizar datos sobre el SGC y mejorar su eficacia. Corregir las no conformidades para prevenir la recurrencia. Promover una cultura de mejora continua de la calidad.

Las actividades que se deben realizar son:

1. Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua.

2. Establecer una plataforma para compartir las mejores prácticas y para capturar la información sobre los defectos y errores que permita aprender de ellos.

3. Identificar ejemplos recurrentes de los defectos de calidad, determinar su causa raíz, evaluar su impacto y resultado y acordar acciones de mejora con todos los miembros de los proyectos y los servicios.

4. Promover una cultura de calidad y mejora continua.

5. Establecer un circuito de retroalimentación entre la gestión de la calidad y la gestión de problemas.

6. Proporcionar a los empleados la formación necesaria en los métodos y herramientas de mejora continua.

7. Realizar un análisis comparativo con los resultados de las revisiones de calidad internas frente a datos históricos, las directrices de la industria, las normas y datos de tipo similar en otras empresas.

Para la monitorización del desarrollo del proceso es necesario que se implanten y se controlen indicadores que permitan conocer el grado de éxito del proceso, y esto se llevará a cabo mediante el registro de ciertas métricas. Algunas de las métricas que se podrían utilizar para evaluar el correcto funcionamiento del proceso son:

- Promedio de satisfacción de las partes interesadas con las soluciones y servicios. Esto se podría medir sacando una media de las partes interesadas que han respondido a una pequeña encuesta donde se pregunte si están satisfechas con las soluciones y servicios.
- Porcentaje de proyectos revisados que cumplen con las metas y objetivos de calidad. Esto se podría medir contando el número de proyectos que cumplen con las metas y objetivos de calidad con respecto de los proyectos revisados totales.

Este proceso tiene sentido desde el punto de vista de que la calidad de los servicios ofrecidos y el aseguramiento de ésta es uno de los factores que diferencia a una organización a la vez de que aseguran la continuidad del negocio. Ahora que APSA va a pivotar en su operativa empresarial, pasando del mundo analógico al digital, en este nuevo escenario no puede permitirse el fallo de que sus servicios no posean al menos la misma calidad que los servicios que venía prestando hasta ahora. Y además debe asegurarse de que, ya sean servicios que se digitalizan o nuevos servicios que aparecen, éstos se presten con un nivel de calidad suficiente, así como también que esta calidad pueda ser medida y controlada fehacientemente.

#### 10.4.5 Proceso de Gestión de Programas y Proyectos

El quinto proceso que debería tener APSA es **Gestión de Programas y Proyectos**. Este proceso pertenece al área de Gestión TI y está dentro del dominio Construir, Adquirir e Implementar. Este proceso sirve para gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa; iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión

post-implementación. Su propósito es alcanzar los beneficios de negocio y reducir el riesgo de retrasos y costes inesperados y el deterioro del valor, mediante la mejora de las comunicaciones y la involucración de usuarios finales y de negocio, asegurando el valor y la calidad de los entregables del proyecto y maximizando su contribución al portafolio de servicios e inversiones.

Este proceso se divide en catorce prácticas que se deberían de realizar:

- La primera de las prácticas es Mantener un enfoque estándar para la gestión de programas y proyectos, es decir, mantener un enfoque estándar para la gestión de programas y proyectos que posibilite revisiones y tomas de decisión de gobierno y de gestión y actividades de gestión de la entrega, enfocadas en la consecución de valor y de objetivos (requisitos, riesgos, costes, cronograma y calidad) para el negocio de una forma consistente.

Las actividades que se deben realizar son:

1. Mantener y reforzar un enfoque estándar de la gestión de programas y proyectos alineado al entorno específico de la empresa y a las buenas prácticas basadas en procesos definidos y el uso de tecnología apropiada. Asegurar que el enfoque cubra todo el ciclo de vida y las disciplinas a utilizar, incluyendo la gestión de alcance, recursos, riesgos, costes, calidad, tiempo, comunicaciones, involucración de las partes interesadas, adquisiciones, control de cambios, integración y generación de beneficios.
2. Actualizar el enfoque de gestión de programas y proyectos sobre la base de las lecciones aprendidas en su uso.

- La segunda de las prácticas es Iniciar un programa, es decir, iniciar un programa para confirmar los beneficios esperados y para obtener la autorización para proceder. Esto incluye los acuerdos sobre el patrocinio del programa, confirmar el mandato del programa a través de la aprobación del caso de negocio conceptual, designar a los consejeros o los miembros del comité del programa, generar el expediente del programa, revisar y actualizar el caso de negocio, desarrollar un plan de realización de beneficios y obtener la aprobación de los patrocinadores para empezar.

Las actividades que se deben realizar son:

1. Acordar el patrocinio del programa y designar una Junta/Comité con miembros que tengan intereses estratégicos en el programa y con responsabilidad en la toma de decisiones de inversión, que serán afectados significativamente por el programa y que serán necesarios para facilitar el cambio.
  2. Confirmar el mandato del programa con los patrocinadores y las partes interesadas. Articular los objetivos estratégicos para el programa, las estrategias potenciales de entrega, las mejoras y los beneficios que se esperan y cómo el programa encaja con otras iniciativas.
  3. Desarrollar un caso de negocio detallado para el programa, si se justifica. Involucrar a todas las partes interesadas relevantes para desarrollar y documentar un entendimiento completo de los resultados esperados por la empresa, cómo serán medidos estos resultados, el alcance total de las iniciativas requeridas, el riesgo involucrado y el impacto en todos los aspectos de la empresa. Identificar y evaluar los cursos de acción alternativos para lograr los resultados esperados por la empresa.
  4. Desarrollar un plan de realización de beneficios que será gestionado durante todo el programa para asegurar que los beneficios planificados siempre tengan propietarios, se logren, sostengan y optimicen.
  5. Preparar y someter a aprobación preliminar el caso de negocio inicial (conceptual) del programa, proporcionando información esencial para la toma de decisiones respecto del propósito, la contribución a los objetivos del negocio, la creación de valor esperado, los márgenes de tiempo, etc.
  6. Designar un gerente dedicado para el programa, con las competencias y habilidades adecuadas para gestionar el programa de forma eficiente y efectiva.
- La tercera de las prácticas es Gestionar el compromiso de las partes interesadas, es decir, gestionar el compromiso de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna, que llegue a todas las partes

interesadas relevantes. Esto incluye la planificación, identificación y el compromiso de las partes interesadas y la gestión de sus expectativas.

Las actividades que se deben realizar son:

1. Planificar la forma en que las partes interesadas internas y externas de la empresa serán identificadas, analizadas, comprometidas, y gestionadas a lo largo del ciclo de vida de los proyectos.
2. Identificar, comprometer y gestionar a las partes interesadas, estableciendo y manteniendo niveles apropiados de coordinación, comunicación y vinculación para asegurar que estén involucrados en los programas/proyectos.
3. Medir la efectividad del compromiso de las partes interesadas y tomar acciones de remediación si es necesario.
4. Analizar los intereses y los requisitos de las partes interesadas.

- La cuarta de las prácticas es Desarrollar y mantener el plan de programa, es decir, formular un programa para definir las bases iniciales y posicionarlo para una ejecución exitosa mediante la formalización del alcance del trabajo a ser efectuado e identificando los entregables que satisfarán sus objetivos y la entrega de valor. Mantener y actualizar el plan del programa y el caso de negocio a lo largo del ciclo de vida económico completo del programa, asegurando el alineamiento con los objetivos estratégicos y reflejando el estado actual y los conocimientos obtenidos hasta el momento.

Las actividades que se deben realizar son:

1. Definir y documentar el plan de programa cubriendo todos los proyectos, incluyendo lo que sea necesario para lograr cambios en la empresa; su imagen, productos y servicios, procesos de negocio, habilidades y cantidad de personal, requerimientos tecnológicos, relaciones con las partes interesadas, clientes, proveedores, entre otros, así como las reestructuraciones organizacionales necesarias para lograr los resultados que la empresa espera del programa.



2. Especificar las habilidades y los recursos necesarios para ejecutar el proyecto, incluyendo los gerentes y los equipos del proyecto, así como los recursos del negocio. Especificar la financiación, coste, cronograma y las interdependencias de los múltiples proyectos. Especificar las bases para la contratación y asignación de miembros del personal competentes y/o contratistas a los proyectos. Definir los roles y las responsabilidades para todos los miembros del equipo y otras partes interesadas.

3. Asignar la responsabilidad ejecutiva para cada proyecto en forma clara y sin ambigüedades, incluyendo el logro de los beneficios, el control de costes, la gestión de riesgos y la coordinación de las actividades de los proyectos.

4. Asegurar que existe una comunicación efectiva de los planes de programa e informes de avance sobre todos los proyectos y con todo el programa. Asegurar que cualquier cambio hecho en los planes individuales se refleje en el resto de planes de programa de la empresa.

5. Mantener el plan de programa para asegurar que esté actualizado y refleje su alineamiento con los objetivos estratégicos actuales, el nivel de avance y los cambios materiales en los resultados, beneficios, costes y riesgos. La empresa tiene que difundir los objetivos y priorizar los trabajos para asegurar que el programa diseñado satisfará los requerimientos de la empresa. Revisar el avance de los proyectos individuales, ajustándolos si fuera necesario para satisfacer las entregas planificadas.

6. Actualizar y mantener el caso de negocio y el registro de beneficios a lo largo de la vida económica del programa para identificar y definir los beneficios principales surgidos de los programas ejecutados.

7. Preparar un presupuesto del programa que refleje los costes del ciclo de vida económico completo, así como los beneficios financieros y no financieros asociados.

- La quinta de las prácticas es Lanzar y ejecutar el programa, es decir, lanzar y ejecutar el programa para adquirir y dirigir los recursos necesarios para lograr las metas y beneficios definidos en el plan del programa. De acuerdo con los criterios de revisión de lanzamiento o cambio de fase (stage-gate), preparar los cambios de fase, las revisiones

de las iteraciones o versiones para informar del progreso del programa y ser capaz de establecer los fundamentos para la financiación de la siguiente etapa después de la revisión del lanzamiento o de cambio de fase (stage-gate).

Las actividades que se deben realizar son:

1. Planificar, dar recursos y asignar las responsabilidades requeridas para los proyectos necesarios para lograr los resultados del programa, basados en las revisiones de financiación y las aprobaciones en cada revisión de cambio de fase (stage-gate).
2. Establecer etapas acordadas para el proceso de desarrollo (puntos de verificación del desarrollo). Al final de cada etapa, facilitar discusiones formales de los criterios aprobados con las partes interesadas. Después de la finalización exitosa de la revisión de funcionalidad, rendimiento y calidad, y antes de finalizar las actividades de la etapa, obtener la aprobación formal y la firma de todas las partes interesadas y del patrocinador/propietario del proceso de negocio.
3. Llevar a cabo un proceso de obtención de beneficios durante el programa para asegurar que los beneficios planeados siempre tienen propietarios y que es probable que se consigan, mantengan y se optimicen. Supervisar la entrega de beneficios e informar con relación a las metas de rendimiento en la revisión de los cambios de fase o de iteración o en las revisiones de lanzamiento. Realizar análisis de causa-raíz para las desviaciones del plan e identificar y tomar las acciones correctivas necesarias.
4. Administrar cada programa o proyecto para asegurar que la toma de decisiones y las actividades de entrega están enfocadas en el valor mediante la consecución de los beneficios y las metas del negocio de una manera consistente, considerando el riesgo y alcanzando los requerimientos de las partes interesadas.
5. Establecer oficina(s) de gestión de programas/proyectos y planificar auditorías, revisiones de calidad, revisiones de cambio de fase (stage-gate) y revisiones de los beneficios realizados.

- La sexta de las prácticas es Supervisar, controlar e informar de los resultados del programa, es decir, supervisar y controlar el rendimiento del programa (entrega de

soluciones) y de la organización (valor/resultado) versus el plan durante el ciclo de vida económico completo de la inversión. Informar del rendimiento al comité estratégico del programa y a los patrocinadores.

Las actividades que se deben realizar son:

1. Supervisar y controlar el rendimiento del programa general y de los proyectos dentro del programa, incluyendo la contribución al negocio y a TI de los proyectos, e informar de una manera oportuna, completa y veraz. Los informes pueden incluir cronogramas, financiación, funcionalidad, satisfacción del usuario, controles internos y aceptación de responsabilidades.
2. Supervisar y controlar el desempeño versus las estrategias y metas de la organización y TI e informar a la dirección de la organización de los cambios implementados, los beneficios logrados versus el plan y la idoneidad del proceso de obtención de beneficios.
3. Supervisar y controlar los servicios, activos y recursos de TI creados o modificados como resultado del programa. Verificar las fechas de implementación y puesta en servicio. Informar a la dirección de los niveles de rendimiento, entrega de servicio sostenido y contribución al valor.
4. Gestionar el desempeño del programa versus criterios claves (por ejemplo, alcance, planificación, calidad, obtención de beneficios, costes, riesgos, rapidez), identificar las desviaciones del plan y tomar oportunamente acciones correctivas cuando sean requeridas.
5. Supervisar el desempeño de proyectos individuales en relación a la entrega de unas esperadas capacidades, planificaciones, beneficios, costes, riesgos u otras métricas para identificar impactos potenciales en el rendimiento del programa. Tomar acciones correctivas oportunas cuando sea requerido.
6. Actualizar los portafolios operacionales de TI que reflejen los cambios que resultan de los programas en los portafolios relevantes de servicios, activos y recursos de TI.

7. Realizar revisiones de acuerdo con los criterios de revisión de cambios de fase (stage-gate), de lanzamiento o de iteración para informar del proceso del programa para que la dirección pueda tomar decisiones de continuar/parar o de ajuste y aprobar financiación adicional para el siguiente cambio de fase, lanzamiento o iteración.

- La séptima de las prácticas es Lanzar e iniciar proyectos dentro de un programa, es decir, definir y documentar la naturaleza y alcance del proyecto para confirmar y desarrollar entre las partes interesadas un entendimiento común o el alcance del proyecto y cómo se relaciona con otros proyectos dentro del programa general de inversiones de TI. La definición debería estar formalmente aprobada por el patrocinador del programa y del proyecto.

Las actividades que se deben realizar son:

1. Crear un entendimiento común del alcance del proyecto entre las partes interesadas, proveer a las partes interesadas de una declaración clara y por escrito que defina la naturaleza, alcance y beneficio de cada proyecto.
2. Asegurar que cada proyecto tenga uno o más patrocinadores con suficiente autoridad para gestionar la ejecución del proyecto dentro los programas generales.
3. Asegurar que las partes interesadas y patrocinadores claves dentro de la organización y TI estén de acuerdo y acepten los requerimientos de los proyectos, incluyendo la definición del criterio de éxito del proyecto (aceptación) y los indicadores claves de desempeño (KPIs).
4. Asegurar que la definición del proyecto describa los requerimientos para el plan de comunicación del proyecto que identifique las comunicaciones del proyecto, tanto internas como externas.
5. Con la aprobación de las partes interesadas, mantener una definición del proyecto durante la vida del proyecto que refleje los cambios en los requerimientos.

6. Hacer un seguimiento de la ejecución del proyecto, poniendo mecanismos tales como informes regulares y revisiones de cambios de estado (stage-gate), lanzamientos o fases de una manera oportuna y con una aprobación adecuada.

- La octava de las prácticas es Planificar proyectos, es decir, establecer y mantener un plan de proyecto formal, aprobado e integrado (que cubra los recursos del negocio y de TI), para guiar la ejecución del proyecto y controlarlo durante toda su vida. El alcance de los proyectos debería estar claramente definido y vinculado claramente a la construcción o aumento de la capacidad del negocio.

Las actividades que se deben realizar son:

1. Desarrollar un plan de proyecto que provea información que permita a la dirección controlar el progreso del proyecto progresivamente. El plan debería incluir detalles de los entregables del proyecto y criterios de aceptación, recursos y responsabilidades requeridas interna y externamente, estructuras claras de división de trabajo y paquetes de tareas, estimaciones de recursos necesarios, hitos/planes de lanzamiento/fases, dependencias claves y la identificación del camino crítico (critical path).
2. Mantener el plan del proyecto y cualquier plan dependiente (por ejemplo, plan de riesgo, plan de calidad, plan de obtención de beneficios) para asegurar que están actualizados y reflejan su progreso real y los cambios materiales aprobados.
3. Asegurar que existe una comunicación efectiva de los planes del proyecto y los informes de progreso dentro de todos los proyectos y dentro del programa general. Asegurar que los cambios hechos a planes individuales son reflejados en otros planes.
4. Determinar las actividades, interdependencias, colaboración necesaria y comunicación dentro de los múltiples proyectos en el programa.
5. Asegurarse que cada hito es acompañado por un entregable significativo que requiere revisión y aprobación.

6. Establecer un marco base del proyecto (por ejemplo, coste, cronograma, alcance, calidad) que es debidamente revisado, aprobado e incorporado en el plan de proyectos integrado.

- La novena de las prácticas es Gestionar la calidad de los programas y proyectos, es decir, preparar y ejecutar un plan y procesos y prácticas de gestión de la calidad, alineadas al SGC que describe el enfoque de calidad del programa y el proyecto y cómo será implementado. El plan debería ser formalmente revisado y acordado por todas las partes afectadas y, después, incorporado en los planes integrados del programa y los proyectos.

Las actividades que se deben realizar son:

1. Identificar las actividades y prácticas de aseguramiento para apoyar la acreditación de sistemas nuevos o modificados durante la planificación del programa y del proyecto e incluirlos dentro de los planes integrados. Asegurarse que las tareas provean garantías de que las soluciones de seguridad y los controles internos cumplen con los requerimientos definidos.

2. Proporcionar garantías de calidad para los entregables del proyecto, identificar a propietarios y responsabilidades, revisar el proceso de calidad, criterios de éxito y las métricas de desempeño.

3. Definir cualquier requerimiento para la validación y verificación independientes de la calidad de los entregables en el plan.

4. Realizar aseguramiento de la calidad y actividades de control de acuerdo con el plan de gestión de la calidad y el SGC.

- La décima de las prácticas es Gestionar el riesgo de los programas y proyectos, es decir, eliminar o minimizar los riesgos específicos asociados con los programas y proyectos mediante un proceso sistemático de planificación, identificación, análisis, respuesta, supervisión y control de las áreas o eventos que tienen el potencial de causar cambios no deseados. Los riesgos enfrentados por la administración del programa y los proyectos deberían ser establecidos y registrados en un único punto.

Las actividades que se deben realizar son:

1. Establecer un enfoque de gestión de riesgo de proyectos alineado con el marco de referencia de ERM. Asegurar que este enfoque incluya la identificación, análisis, respuesta, mitigación, supervisión y control del riesgo.
  2. Asignar la responsabilidad para ejecutar el proceso de gestión del riesgo de los proyectos de la entidad al personal con las capacidades adecuadas y asegurar que está incorporado en las prácticas de desarrollo de la solución. Considerar asignar este perfil a un equipo independiente, especialmente si es necesario un punto de vista objetivo o el proyecto se considera crítico.
  3. Realizar un análisis de riesgo del proyecto para identificar y cuantificar el riesgo de manera continua durante el proyecto. Gestionar y comunicar el riesgo adecuadamente dentro de la estructura de gobierno del proyecto.
  4. Reevaluar el riesgo del proyecto periódicamente, incluyendo al inicio de cada fase de un proyecto importante y como parte de las evaluaciones de solicitudes de cambios importantes.
  5. Identificar los propietarios de las acciones para evitar, aceptar o mitigar el riesgo.
  6. Mantener y revisar el registro de los riesgos potenciales del proyecto y el registro de la mitigación de riesgos de todos los aspectos del proyecto y su resolución. Analizar periódicamente el registro para ver tendencias y problemas recurrentes y asegurarse que se corrigen las causas raíz.
- La onceava práctica es Supervisar y controlar proyectos, es decir, medir el desempeño del proyecto versus los criterios clave de rendimiento del proyecto, tales como la planificación, la calidad, el coste y los riesgos. Evaluar el impacto de las desviaciones en el proyecto y el programa general e informar los resultados a las partes interesadas clave.

Las actividades que se deben realizar son:

1. Establecer y usar un conjunto de criterios de proyecto que incluyan, pero no limitados a, alcance, planificación, calidad, coste y nivel de riesgo.
2. Medir el rendimiento del proyecto versus criterios claves de rendimiento. Analizar las desviaciones de criterios claves de desempeño por su causa y evaluar los efectos positivos y negativos en el programa y los proyectos que lo componen.
3. Notificar el progreso del proyecto dentro del programa, las desviaciones de los criterios claves de desempeño establecidos y los efectos positivos y negativos en los programas y en los proyectos que los componen a las partes interesadas identificadas como claves.
4. Supervisar los cambios al programa y revisar los criterios claves de desempeño del proyecto para determinar si estos representan medidas válidas del avance.
5. Documentar y enviar cualquier cambio al programa a las partes interesadas claves antes de su adopción. Comunicar los criterios revisados a los jefes de proyecto para su uso en los informes futuros de desempeño.
6. Recomendar y supervisar las acciones correctivas, cuando sean requeridas, en línea con el marco de gobierno de programas y proyectos.
7. Obtener la aprobación y firma documentada de los entregables producidos en cada iteración, lanzamiento o fase del proyecto de los gestores y usuarios designados que afectan las funciones del negocio y a TI.
8. Basar el proceso de aprobación en criterios de aceptación claramente definidos y acordados con las partes interesadas claves antes de que comience el trabajo sobre el entregable de la fase o de la iteración.
9. Evaluar el proyecto en los cambios de fase (stage-gate), versiones o iteraciones más importantes acordados y tomar la decisión de continuar/parar de acuerdo con criterios de éxito predeterminados.
10. Establecer y operar un sistema de control de cambios para el proyecto de forma que todos los cambios a la línea de referencia (baseline) del proyecto (por ejemplo, coste,



cronograma, alcance, calidad) sean adecuadamente revisados, aprobados e incorporados en el plan de proyecto integrado en línea con el marco de gobierno del programa y proyectos.

- La doceava de las prácticas es Gestionar los recursos y los paquetes de trabajo del proyecto, es decir, gestionar los paquetes de trabajo mediante requerimientos formales de autorización y aceptación de los paquetes de trabajo, y asignando y coordinando los recursos de negocio y de TI adecuados.

Las actividades que se deben realizar son:

1. Identificar las necesidades de recursos del negocio y TI para el proyecto y mapear claramente los perfiles y responsabilidades, con las responsabilidades para la escalado y la toma de decisiones que han sido acordadas y entendidas.
2. Identificar los requerimientos de habilidades y tiempo para todos los individuos involucrados en las fases del proyecto con relación a sus perfiles definidos. Asignar personal a los roles basándose en la información sobre las habilidades disponibles (p.ej. matriz de habilidades de TI).
3. Utilizar un gestor de proyecto experimentado y un líder de equipo con habilidades apropiadas al tamaño, complejidad y riesgo del proyecto.
4. Considerar y definir claramente los roles y responsabilidades de otras partes involucradas, incluyendo financiero, legal, compras, RRHH, auditoría interna y cumplimiento.
5. Definir y acordar claramente la responsabilidad sobre la compra y gestión de productos y servicios de terceras partes, así como la gestión de las relaciones.
6. Identificar y autorizar la ejecución del trabajo de acuerdo al plan de proyecto.
7. Identificar las diferencias con el plan de proyecto y dar realimentación al jefe de proyecto para su remediación.

- La treceava de las prácticas es Cerrar un proyecto o iteración, es decir, solicitar a las partes interesadas del proyecto, al final de cada proyecto, versión o iteración, que evalúen si el proyecto, la versión o la iteración entregaron los resultados y valor planeados. Identificar y comunicar cualquier actividad pendiente necesaria para lograr los resultados del proyecto y los beneficios del programa planeados, identificar y documentar las lecciones aprendidas para futuros proyectos, versiones, iteraciones y programas.

Las actividades que se deben realizar son:

1. Definir y aplicar los pasos claves para el cierre del proyecto, incluyendo revisiones post-implementación que evalúen si el proyecto obtuvo los resultados y beneficios deseados.
2. Planificar y ejecutar revisiones post-implementación para determinar si los proyectos entregaron los beneficios esperados y para mejorar la metodología de gestión de proyecto y el proceso de desarrollo de sistemas.
3. Identificar, asignar, comunicar y rastrear las actividades incompletas necesarias para lograr los resultados y beneficios planeados del programa del proyecto.
4. Recolectar las lecciones aprendidas de los participantes del proyecto regularmente y hasta la finalización del proyecto. Revíselas e identifique las actividades claves que llevaron a los beneficios y valor entregados. Analice los datos y haga recomendaciones para mejorar los proyectos actuales, así como el método de gestión para proyectos futuros.
5. Obtenga la aceptación de los entregables y la transferencia de propiedad del proyecto de las partes interesadas.

- La catorceava de las prácticas es Cerrar un programa, es decir, eliminar el programa del portafolio de inversiones activas cuando haya acuerdo de que el valor deseado ha sido logrado o cuando esté claro que no será logrado con los criterios de valor establecidos para el programa.

Las actividades que se deben realizar son:

1. Llevar el programa a un cierre ordenado, incluyendo una aprobación formal, desmantelamiento de la organización del programa y la función de apoyo, validación de los entregables y comunicación de la retirada.
2. Revisar y documentar las lecciones aprendidas. Una vez que el programa ha sido retirado, elimínalo del portafolio de inversiones activas.
3. Establecer la responsabilidad y los procesos para asegurar que la organización continúe la optimización del valor de los servicios, activos o recursos. Pueden ser necesarias inversiones adicionales en el futuro para asegurarse que esto ocurra.

Para la monitorización del desarrollo del proceso es necesario que se implanten y se controlen indicadores que permitan conocer el grado de éxito del proceso, y esto se llevará a cabo mediante el registro de ciertas métricas. Algunas de las métricas que se podrían utilizar para evaluar el correcto funcionamiento del proceso son:

- Nivel de satisfacción con la involucración de las partes interesadas. Esto se podría medir realizando una encuesta y preguntando a la directiva por el nivel de satisfacción con la involucración de las partes interesadas.
- Porcentaje de desviaciones del plan de referencia. Esto se podría medir contando cuantos proyectos se desvían del plan de referencia con respecto al total que hay en plan de referencia.
- Porcentaje de beneficios esperados que se han alcanzado. Esto se podría medir viendo cuál es el total de beneficios esperados y cuáles se han alcanzado realmente.

Este proceso tiene sentido desde el punto de vista de que, para poder lograr sus objetivos van a tener que controlar que todos los proyectos y programas vayan de forma coordinada y que se alineen con la estrategia corporativa. Si bien la gestión del portafolio asegura que los nuevos servicios a desarrollar se alineen con el negocio, este proceso asegura que al desarrollar los proyectos del portafolio no se deteriora el valor de los ya desarrollados o de los futuros por desarrollar, además de que todas las partes

interesadas conocen el valor generado y que la entrega se realiza a todas las partes, ya sean del negocio o los usuarios finales.

#### 10.4.6 Métricas TI

Una vez descritos detalladamente todos los procesos y que métricas de negocio podrían emplearse para saber si el proceso está funcionando correctamente, vamos a ver algunas métricas que podrían emplearse para evaluar el correcto cumplimiento de las Metas TI. No hay que olvidar que cada proceso (o catalizador COBIT) se implementa con el objetivo de alcanzar el cumplimiento de ciertas metas TI, es decir, el objetivo no es implementar los procesos sino implementar los procesos para lograr cumplir con las metas TI (que a su vez persiguen potenciar el cumplimiento de las metas de negocio o corporativas), por ello es importante también tener alguna herramienta (en este caso en forma de métrica) sobre el éxito o no de las metas TI, por lo que:

- Para evaluar la meta Alineamiento de TI y estrategia de negocio, se podría usar la métrica de porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI y para ello se debería ver que metas y requerimientos estratégicos de la Asociación son soportados por las metas estratégicas para TI sobre el total de metas y requerimientos estratégicos.
- Para evaluar la meta Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI, se podría usar la métrica de porcentaje de los servicios TI en los que se realizan los beneficios esperados, ya que el beneficio esperado se ha estimado y se puede fácilmente comprobar si se están o no logrando los beneficios.
- Para evaluar la meta Entrega de servicios de TI de acuerdo a los requisitos del negocio, se podría usar la métrica de número de interrupciones del negocio debidas a incidentes en el servicio de TI y para ello se debería monitorizar en algún sitio cuando se interrumpe el negocio debido a incidentes en el servicio de TI. También sería importante utilizar la monitorización del porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados, por lo que se monitorizaría esta variable también mediante pequeñas encuestas de satisfacción.

- Para evaluar la meta Optimización de activos, recursos y capacidades de las TI, se podría usar la métrica frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes para ver con qué frecuencia se evalúa la madurez de la capacidad TI y de la optimización de costes (por ejemplo 1 vez al año) y para ello se debería registrar en algún sitio cuantas veces al año se evalúan estas dos cosas.
- Para evaluar la meta Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad, se podría usar la métrica coste del mantenimiento de aplicaciones respecto al coste total de TI y para ello debería quedar registrado cuál es el coste del mantenimiento de aplicaciones en un año con respecto al coste total de TI.

Cascada de Metas APSA

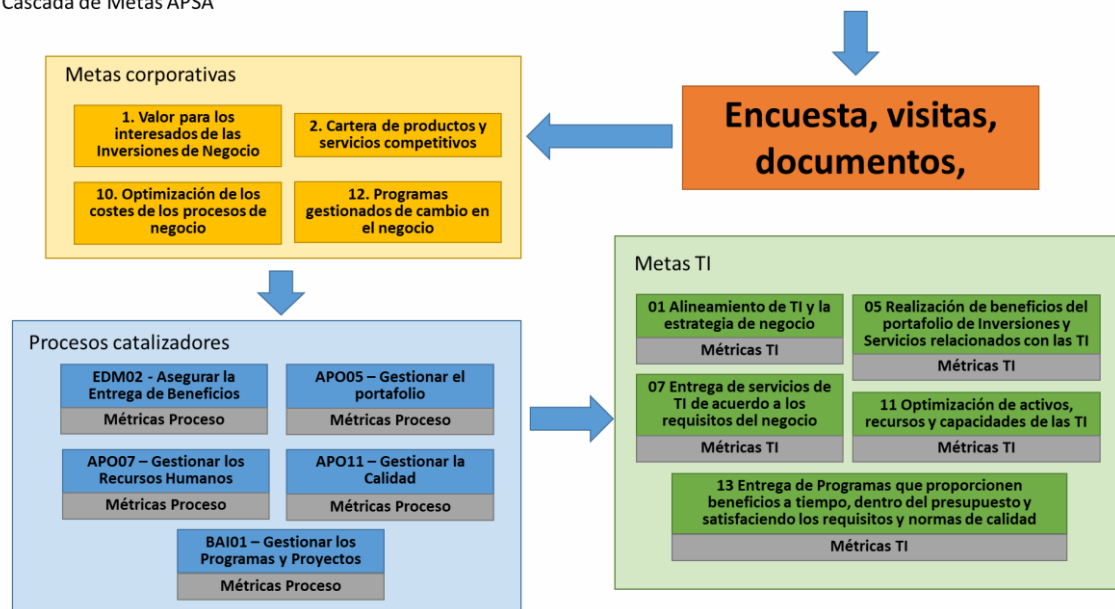


Ilustración 19. Cascada de metas APSA

(Fuente propia)

#### 10.4.7. Acciones a corto plazo

Mientras que la implementación de los procesos COBIT descritos tienen como objetivo el asegurar que tanto TI como metas corporativas estarán alineadas y correctamente implementadas, tras la auditoría de la empresa vamos a realizar una serie de recomendaciones que deberían ser implantadas en un tiempo relativamente corto

(entre 1 semana y 3 meses) para resolver las cuestiones más acuciantes, así como también recomendaciones de mejoras a más largo plazo.

Del cuestionario correspondiente al área de planificación, deberíamos recomendar como acciones necesarias que:

- Se haga entender que la TI es un valor para la asociación y que la dirección general y ejecutiva debería considerar la importancia que tiene el estudio del sistema de información.
- Se piense en requisitos de información a largo plazo para así prever mejor las acciones que se deben tomar ya que, así los cambios en los sistemas informáticos no serían consecuencia de la presión por necesidades operativas.
- Se debería realizar una planificación estratégica del sistema de información ya que, como hemos comentado anteriormente este es valor para la asociación.

Como acciones para una mejora a más largo plazo:

- Se debería considerar, al menos en el departamento TI, la evolución del mercado para así poder estar al día y poder adecuar sus servicios al mercado.

Del cuestionario correspondiente a los dispositivos de almacenamiento, deberíamos recomendar que:

- Se debe gestionar mejor el inventario, puesto que actualmente éste se realiza mediante varios documentos Excel y se debería utilizar un programa de código abierto de gestión de inventario como podrían ser GLPi o Odoo.
- Se debe controlar que si se destruye un archivo por equivocación se pueda recuperar.
- Se deben realizar auditorías periódicas a los medios de almacenamiento para comprobar el correcto funcionamiento de éstos.
- Cuando se reemplace una cinta por otra sea controlada por alguno de los trabajadores del departamento TI.

- Cuando haya archivos que se manejen archivos en línea haya procedimientos para recuperar los archivos y que los conozcan los trabajadores del departamento TI.

Como acciones para una mejora a más largo plazo:

- Los servidores de datos deberían tener protección automática contra el fuego.
- Debería haber un responsable de los servidores por cada turno ya que, en los servidores se encuentra la información sensible de la asociación.
- Se debería llevar un control sobre los archivos que se prestan para si en algún momento se necesitan y no se encuentran saber si han sido prestados y a quién.
- Se conserve la cinta maestra anterior hasta que haya una nueva cinta por si hubiera algún problema y se tuviera que recuperar la información.
- Se debería tener un procedimiento bien estructurado para el manejo de la información del *cuarto frío* que conozcan los trabajadores del departamento TI.
- Se distribuyan de forma periódica entre los trabajadores del departamento TI informes de archivos para que se liberen los dispositivos de almacenamiento.

Del cuestionario correspondiente al funcionamiento del centro de cómputo, deberíamos recomendar que:

- Haya lugar suficiente para los equipos ya que si no hay espacio suficiente para esto no se pueden ofrecer debidamente los servicios.
- Se debería controlar la temperatura para que sea adecuada a las normas bajo las cuales se rige.
- Se debería disponer de aire acondicionado para que los servidores estén a la temperatura adecuada.
- Se debería disponer de un switch de apagado para poder usarlo en caso de emergencia y que no haya problemas de pérdida de información o de fallo en los equipos.
- Se debería contar con alarma contra inundaciones.

- Se debería disponer de un control de entradas y salidas de usuario para que no pudieran acceder usuarios no autorizados y tener un control en caso de que fallara algo.

Como acciones para una mejora a más largo plazo:

- El material con que está construido el centro de cómputo sea confiable.
- Se debería contar con un equipo interrumpible.
- Se debería contar con manuales para cada programa de los que se manejan y que los trabajadores del departamento TI supieran el contenido de éstos.
- Se debería intentar realizar un mantenimiento de los programas preventivo para no tener que ir corrigiendo las necesidades detectadas y así tener un mejor funcionamiento.

Del cuestionario correspondiente a la seguridad física, deberíamos recomendar que:

- Se deberían adoptar medidas de seguridad en el departamento de sistemas de información.
- Debería haber personal de vigilancia en la institución o al menos debería haber cámaras de seguridad para poder controlar lo que sucede. Así como también la debería haber en el centro de cómputo.
- Se debería tener claro que función o funciones tiene cada uno de los puestos clave.
- Se debería controlar el trabajo fuera de horario.
- El edificio donde se encuentra el centro de cómputo debería estar a salvo de, como mínimo, una de estas cosas: inundación, terremoto, fuego, sabotaje.
- Se debería registrar el acceso al centro de cómputo de personas ajenas al departamento TI, así como controlar las visitas y demostraciones en éste.
- Se debería tener alarma en las instalaciones para detectar fuego o humo de forma automática y para detectar una fuga de agua.



Como acciones para una mejora a más largo plazo:

- Se debería registrar las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas.
- Se debería instruir a los trabajadores del departamento TI sobre qué medidas deben tomar en caso de que alguien pretenda entrar sin autorización a los archivos y programas.
- Los interruptores de energía deberían estar debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos.

## 11.- Resultados

A modo de síntesis del trabajo realizado, en esta sección se resumirán los principales resultados obtenidos de este trabajo.

En primer lugar, se ha creado, tras una revisión del estado del arte y análisis de las mecánicas de auditoría TI, una metodología de análisis TI mediante la cual hemos establecidos una serie de herramientas y procesos para generar una auditoría TI, creando lo que se denomina Plan Auditor. Este Plan Auditor se estructura en 4 grandes procesos:

- **Análisis:** en esta fase se idéntica el origen o necesidad de la auditoría, se determinan los objetivos y se conoce y estudia la empresa en general.
- **Planificación:** en esta fase se determinan los puntos de la empresa a ser evaluados respecto a la TI después del análisis inicial, se identifican y seleccionan los métodos, herramientas, instrumentos y procedimientos necesarios, y se elaboran los planes y programas para la auditoría junto la asignación de recursos.
- **Ejecución:** fase en la que se llevan a cabo las actividades de recopilación de información mediante las herramientas establecidas, hasta encontrar el punto de satisfacción por las partes implicadas.
- **Dictamen:** fase final en la que, a partir de la información obtenida, se emiten las recomendaciones para la empresa para proporcionarles una mejora en el alineamiento entre empresa y TI a la vez que intentar asegurar el buen gobierno y gestión TI.

La segunda gran aportación ha sido instanciar este plan auditor a un caso real, el análisis de la Asociación APSA que en estos momentos desarrolla un importante proceso de digitalización de sus servicios actuales y generación de nuevos servicios. Esta situación obliga a realizar una reflexión ya que la actividad de la empresa tendrá como eje principal la TI y es un momento delicado donde las decisiones actuales pueden marcar el rumbo futuro de la asociación.

Dentro de la instanciación del plan auditor se han establecido dos herramientas para realizar el análisis. Por un lado, se ha creado un cuestionario propio para la captación de información, focalizado en los puntos a analizar por esta auditoría. Los cuestionarios que se utilizan en auditoría TI deben ser personalizados a las características y necesidades de la empresa, y por ello se ha creado uno explícito en este trabajo que recopila información sobre la planificación TI de la empresa, y sobre cuestiones relacionadas con los dispositivos, centro de cómputo y seguridad física, las áreas de estudio que se han determinado en esta auditoría TI. Y por otro lado se ha utilizado COBIT y la cascada de metas como artefacto de análisis de las necesidades principales para un buen gobierno y gestión de la TI, extrayendo cuales son las actividades y procesos más acuciantes a ser implantados por la empresa una vez que han podido ser detectadas cuáles son sus necesidades. El cuestionario se ha puesto además publicado en el repositorio institucional de la Universidad de Alicante y ha sido descargado casi 20 veces y el doble de accesos.

En tercer lugar, y más importante, se ha ejecutado el plan auditor y se ha generado un dictamen en el cual la empresa tiene una serie de recomendaciones basadas en el análisis formal de las actuales características de la empresa y sus necesidades que le permite establecer mecanismos a nivel organización y operativos para asegurar un buen gobierno y gestión de la TI, ya que de ahora en adelante la tecnología será uno de los elementos principales de la empresa.

## 12.- Conclusiones y trabajo futuro

Para concluir este Trabajo de Fin de Grado, me gustaría comentar mi experiencia realizándolo. Primeramente decir que, ha sido un trabajo mucho más difícil de lo que en un principio me esperaba, puesto que el desconocimiento sobre cómo realizar una Auditoría TI me ha llevado a tener que buscar mucha información acerca de ello para poder llegar a realizar este TFG y ha sido un trabajo costoso, donde he tenido que leer una gran cantidad de información que luego he tenido que clasificar según la cantidad de información que me aportaba. Seguidamente, comentar que, el hecho de realizar el TFG en una Asociación real no siempre ha sido fácil puesto que dependes de los datos que ellos te aportan para realizarlo. Finalmente, comentar que, a pesar de que haya sido un trabajo costoso y duro por la falta de conocimiento previo y por todo lo que supone realizar una Auditoría TI en una empresa, en este caso una asociación real, me ha gustado mucho tener la oportunidad de hacer algo así y de poder entender que se debe realizar para evaluar el correcto funcionamiento de la TI en una empresa, además de servirme para salir de mi zona de confort y enfrentarme a un proyecto no simulado, alejado de las prácticas de las asignaturas que son guiadas y enfrentarme a un aprendizaje muy distinto.

Como trabajo futuro quedaría hacer un seguimiento de cuáles son las recomendaciones que se han implantado y si la Asociación ha seguido el consejo de implantación de los cinco procesos que se ha determinado que deben tener para poder cumplir con sus objetivos. Además, se podría ampliar el análisis para establecer más procesos recomendables en función de los intereses de la asociación hasta lograr una gestión y gobierno TI completos.

## Glosario

En esta sección se recogen la descripción de las siglas utilizadas en el trabajo.

ADSL: acrónimo en inglés de Asymmetric Digital Subscriber Line, es un tipo de tecnología de línea de abonado digital.

ANS: Acuerdo de Nivel de Servicio

Backup: copia de seguridad o de respaldo

CDIAT: Centro de Desarrollo Infantil y Atención Temprana

CFP: Centro de Formación Permanente

CIO: Chief Information Officer

C.O: Centro Ocupacional

COFAL: Centro de Orientación, Formación y Asesoramiento Laboral

CRAE: Centro de Recursos y Apoyo Escolar

DAFO: Debilidades, Amenazas, Fortalezas y Oportunidades

DEF: Demandantes de Empleo y Formación

ENL: Entidad No Lucrativa.

ERE: Expediente de Regulación de Empleo

ERM: Marco de referencia

ERP: Enterprise Resource Planning o Planeamiento de Recursos Empresariales

Férulas: adaptaciones ortopédicas

FOL: Formación y Orientación Laboral

GUS: Gestión de Usuarios Socios

G2K: Sistema de Gestión que forma parte de los ERP

Holístico: Del todo o que considera algo como un todo.

IRR: tasa interna de retorno

ISBN: Número de publicación de un libro

KPIs: indicadores claves de desempeño

LOPD: Ley Orgánica de Protección de Datos

NPV: Valor actual neto

ONG: Organización No Gubernamental

PAI: Programa de Apoyo Individual

PCPI: programas de cualificación profesional inicial

PDID: persona con discapacidad intelectual o del desarrollo

PYME's: Pequeñas y medianas empresas

RIS: Registro Individual de Seguimiento

ROI: Retorno de la inversión

RSC: responsabilidad social.

SAE: Servicio de Apoyo Educativo

SAI: Sistema de Alimentación Ininterrumpida

SGC: Sistema de Gestión de Calidad

SIM: acrónimo en inglés de subscriber identity module, en español módulo de identificación de abonado. Es una tarjeta inteligente desmontable usada en teléfonos móviles y módems HSPA o LTE que se conectan al dispositivo por medio de una ranura lectora.

SMART: específicos, medibles, realizables, pertinentes y de duración determinada

SSII: Sistemas de Información

SS.SS: Servicios Sociales

TI: Tecnologías de la información

## Referencias, bibliografía y apéndices

- [1] <http://www.ymant.com/la-funcion-del-cio-en-la-empresa/>
- [2] <http://tecnologiaparatuempresa.ituser.es/transformacion-digital/2017/08/pasos-para-abordar-un-plan-de-digitalizacion> 24 AGO 2017
- [3] VALENZUELA RODRÍGUEZ, JUAN ALONSO  
<http://www.grandespymes.com.ar/2011/06/19/las-tecnologias-de-informacion-en-las-pymes/>
- [4] [https://es.wikipedia.org/wiki/Auditor%C3%ADa\\_inform%C3%A1tica](https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica)
- [5] CYNTHUS <https://www.cynthus.com.mx/blog/auditoria-y-consultoria/auditoria-en-ti/> 27 AGO 2017
- [6] ISACA, COBIT 5: *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*, 2012
- [7] ISACA, COBIT 5: *Procesos Catalizadores*, 2012
- [8] VAN BON, Jan. DE JONG, Argen. KOLTHOF, Axel. PIEPER, Mike. TJASSING, Ruby. VAN DER VEEN, Annalies. VERHEIJEN, Tienieke. *Estrategia del Servicio Basada en ITIL® V3 - Guía de Gestión*
- [9] VAN BON, Jan. DE JONG, Argen. KOLTHOF, Axel. PIEPER, Mike. TJASSING, Ruby. VAN DER VEEN, Annalies. VERHEIJEN, Tienieke. *Diseño del Servicio Basada en ITIL® V3 - Guía de Gestión*
- [10] VAN BON, Jan. DE JONG, Argen. KOLTHOF, Axel. PIEPER, Mike. TJASSING, Ruby. VAN DER VEEN, Annalies. VERHEIJEN, Tienieke. *Transición del Servicio Basada en ITIL® V3 - Guía de Gestión*
- [11] VAN BON, Jan. DE JONG, Argen. KOLTHOF, Axel. PIEPER, Mike. TJASSING, Ruby. VAN DER VEEN, Annalies. VERHEIJEN, Tienieke. *Organización del Servicio Basada en ITIL® V3 - Guía de Gestión*
- [12] VAN BON, Jan. DE JONG, Argen. KOLTHOF, Axel. PIEPER, Mike. TJASSING, Ruby. VAN DER VEEN, Annalies. VERHEIJEN, Tienieke. *Mejora Continua del Servicio Basada en ITIL® V3 - Guía de Gestión*
- [13] AENOR, UNE-ISO/IEC 38500, OCT 2012
- [14] JULIÁ, Samuel. <http://www.gadae.com/blog/guia-para-hacer-una-auditoria->

[informatica-en-tu-empresa/](#)

[15] CORONADO, David <https://prezi.com/tklqkzgttqpt/como-hacer-una-auditoria-informatica> 28 NOV 2012

[16] SOLARTE SOLARTE, Francisco Nicolás  
<http://auditordesistemas.blogspot.com.es/2011/11/metodologia-para-realizar-auditoria.html> 30 NOV 2011

[17] <https://www.mindomo.com/es/mindmap/pasos-para-una-auditoria-en-sistemas-6e885a6d069b4797932170fb0bd7b7ca>

[18] <https://es.scribd.com/doc/18565564/CUESTIONARIO-PARA-REALIZAR-UNA-AUDITORIA-INFORMATICA>

[19] PIATTINI VELTHUIS, M. G., PESO NAVARRO, E. D., & Peso, M. D. (2008). Auditoría de tecnologías y sistemas de información (No. Sirsi) i9789701513781 T58. 5). Auditoría de Tecnologías y Sistemas de Información (Mario Piattini Velthuis, Emilio del Peso Navarro y Mar del Peso Ruiz)

[20] [https://www.odoo.com/es\\_ES/page/warehouse](https://www.odoo.com/es_ES/page/warehouse)

[21] <https://www.erp5.com/feature/inventory>

[22] <https://erpnext.com/features>

[23] PINK, Kathy <http://wiki.compiere.com/display/docs/Material+Management>  
19 AGO 2010

[24] <https://xtuple.com/products/comparison/inventory>

[25] <http://glpi-project.org/>

[26] González Mataix, P. Berná Martínez, J.V. (2018) Cuestionario para auditoría TI. Disponible online en <http://hdl.handle.net/10045/76667>



## Apéndice I

En la primera figura, que se muestra a continuación, se muestra la tabla con los objetivos de la empresa más comunes, dividiéndose la tabla entre dimensión CMI a la cual se ajusta la meta corporativa, las metas corporativas y la relación con las tres metas de gobierno principales.

Dimensión del CMI	Objetivo de la Empresa	Relación con los Objetivos de Gobierno		
		Realización de Beneficios	Optimización de Riesgos	Optimización de Recursos
Financiera	1. Valor para las Partes Interesadas de las Inversiones de Negocio	P		S
	2. Cartera de productos y servicios competitivos	P	P	S
	3. Riesgos de negocio gestionados (salvaguarda de activos)		P	S
	4. Cumplimiento de leyes y regulaciones externas		P	
	5. Transparencia financiera	P	S	S
Cliente	6. Cultura de servicio orientada al cliente	P		S
	7. Continuidad y disponibilidad del servicio de negocio		P	
	8. Respuestas ágiles a un entorno de negocio cambiante	P		S
	9. Toma estratégica de Decisiones basada en Información	P	P	P
	10. Optimización de costes de entrega del servicio	P		P
Interna	11. Optimización de la funcionalidad de los procesos de negocio	P		P
	12. Optimización de los costes de los procesos de negocio	P		P
	13. Programas gestionados de cambio en el negocio	P	P	S
	14. Productividad operacional y de los empleados	P		P
	15. Cumplimiento con las políticas internas		P	
Aprendizaje y Crecimiento	16. Personas preparadas y motivadas	S	P	P
	17. Cultura de innovación de producto y negocio	P		

*Ilustración 20. Objetivos de la empresa*

(COBIT 5 – Procesos Catalizadores)

En la segunda figura, que se muestra a continuación, se muestra la tabla con los objetivos de las TI más comunes.

Dimensión del CMI TI	Objetivo de Información y Tecnología relacionada	
Financiera	01	Alineamiento de TI y estrategia de negocio
	02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
	03	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI
	04	Riesgos de negocio relacionados con las TI gestionados
	05	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI
	06	Transparencia de los costes, beneficios y riesgos de las TI
Cliente	07	Entrega de servicios de TI de acuerdo a los requisitos del negocio
	08	Uso adecuado de aplicaciones, información y soluciones tecnológicas
Interna	09	Agilidad de las TI
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
	11	Optimización de activos, recursos y capacidades de las TI
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
	14	Disponibilidad de información útil y relevante para la toma de decisiones
	15	Cumplimiento de las políticas internas por parte de las TI
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio

*Ilustración 21. Objetivos de las TI*

(COBIT 5 – Procesos Catalizadores)

En la tercera figura, mostrada a continuación, podemos ver una muestra de métricas de las metas corporativas. La información se divide en dimensión del CMI, meta corporativa y métrica.

Dimensión CMI	Meta Corporativa	Métrica
Financiera	1. Valor para las partes interesadas de las Inversiones de Negocio	<ul style="list-style-type: none"> <li>• Porcentaje de inversiones en las que la entrega cumple con las expectativas de los interesados</li> <li>• Porcentaje de productos y servicios en los que se realizan los beneficios esperados</li> <li>• Porcentaje de inversiones en los que se cumplen o superan los beneficios establecidos</li> </ul>
	2. Cartera de productos y servicios competitivos	<ul style="list-style-type: none"> <li>• Porcentaje de productos y servicios que alcanzan o exceden los objetivos de ingresos y/o cuota de mercado</li> <li>• Relación de productos y servicios por fase del ciclo de vida</li> <li>• Porcentaje de productos y servicios que alcanzan o exceden los objetivos de satisfacción al cliente</li> <li>• Porcentaje de productos y servicios que proporcionan ventaja competitiva</li> </ul>
	3. Riesgos de negocio gestionados (salvaguarda de activos)	<ul style="list-style-type: none"> <li>• Porcentaje de objetivos de negocio críticos y servicios cubiertos por gestión del riesgo</li> <li>• Relación de incidentes significativos que no fueron identificados en las evaluaciones de riesgo respecto al número total de incidentes</li> <li>• Frecuencia de actualización del perfil de riesgos</li> </ul>
	4. Cumplimiento de leyes y regulaciones externas	<ul style="list-style-type: none"> <li>• Coste de incumplimientos regulatorios incluyendo acuerdos y sanciones</li> <li>• Número de incumplimientos regulatorios causantes de comentarios públicos o publicidad negativa</li> <li>• Número de incumplimientos regulatorios en relación con acuerdos contractuales con socios de negocios</li> </ul>
	5. Transparencia financiera	<ul style="list-style-type: none"> <li>• Porcentaje de casos de negocio de inversión con costes y beneficios esperados claramente definidos y aprobados</li> <li>• Porcentaje de productos y servicios con costes operativos y beneficios esperados definidos y aprobados</li> <li>• Encuestas de satisfacción a interesados clave en relación con la transparencia, comprensión y precisión de la información financiera corporativa</li> <li>• Porcentaje del coste del servicio que puede ser asignado a usuarios</li> </ul>
Cliente	6. Cultura de servicio orientada al cliente	<ul style="list-style-type: none"> <li>• Número de trastornos del servicio al cliente debidos a incidentes relacionados con el servicio TI (fiabilidad)</li> <li>• Porcentaje de interesados del negocio que se encuentran satisfechos con que la entrega del servicio de cliente cumpla con los niveles acordados</li> <li>• Número de quejas de clientes</li> <li>• Tendencia de los resultados de las encuestas de satisfacción al cliente</li> </ul>

Dimensión CMI	Meta Corporativa	Métrica
Cliente (cont.)	7. Continuidad y disponibilidad del servicio de negocio	<ul style="list-style-type: none"> <li>Número de interrupciones de servicio al cliente causantes de incidentes significativos</li> <li>Coste de negocio de los incidentes</li> <li>Número de horas de procesamiento perdidas debido a interrupciones del servicio no planificadas</li> <li>Porcentaje de quejas en función de los objetivos de disponibilidad del servicio comprometidos</li> </ul>
	8. Respuestas ágiles a un entorno de negocio cambiante	<ul style="list-style-type: none"> <li>Nivel de satisfacción del Consejo de Administración con la capacidad de respuesta corporativa a nuevos requerimientos</li> <li>Número de productos y servicios críticos sustentados por procesos de negocio actualizados</li> <li>Tiempo medio de conversión de objetivos estratégicos corporativos en iniciativas acordadas y aprobadas</li> </ul>
	9. Toma estratégica de Decisiones basada en Información	<ul style="list-style-type: none"> <li>Grado de satisfacción del Consejo de Administración y la alta dirección con la toma de decisiones</li> <li>Número de incidentes causados por decisiones de negocio incorrectas basadas en información imprecisa</li> <li>Tiempo requerido para ofrecer información de apoyo que permita decisiones de negocio efectivas</li> </ul>
	10. Optimización de costes de entrega del servicio	<ul style="list-style-type: none"> <li>Frecuencia de las evaluaciones de optimización del coste de entrega del servicio</li> <li>Tendencia de la evaluación de costes respecto a los resultados del nivel de servicio</li> <li>Niveles de satisfacción del Consejo de Administración y la alta dirección con el coste de entrega del servicio</li> </ul>
Interna	11. Optimización de la funcionalidad de los procesos de negocio	<ul style="list-style-type: none"> <li>Frecuencia de las evaluaciones de madurez de la capacidad de los procesos de negocio</li> <li>Niveles de satisfacción del Consejo de Administración y la alta dirección con las capacidades de los procesos de negocio</li> </ul>
	12. Optimización de los costes de los procesos de negocio	<ul style="list-style-type: none"> <li>Frecuencia de evaluaciones de optimización de costes de los procesos de negocio</li> <li>Tendencia de la evaluación de costes respecto a los resultados del nivel de servicio</li> <li>Niveles de satisfacción del Consejo de Administración y la alta dirección con los costes de procesamiento del negocio</li> </ul>
	13. Programas gestionados de cambio en el negocio	<ul style="list-style-type: none"> <li>Número de programas cumplidos en tiempo y en presupuesto</li> <li>Porcentaje de interesados satisfechos con la ejecución y resultados del programa</li> <li>Nivel de concienciación de cambios en el negocio inducidos por TI Iniciativas de negocio posibilitadas</li> </ul>
	14. Productividad operacional y de los empleado	<ul style="list-style-type: none"> <li>Número de programas/proyectos en tiempo y presupuesto</li> <li>Niveles de coste y de personal comparados con los análisis comparativos</li> </ul>
	15. Cumplimiento con las políticas internas	<ul style="list-style-type: none"> <li>Número de incidentes relacionados con el incumplimiento de políticas</li> <li>Porcentaje de interesados que entienden las políticas</li> <li>Porcentaje de políticas apoyadas por estándares y prácticas de trabajo efectivos</li> </ul>
Aprendizaje y Crecimiento	16. Personas preparadas y motivadas	<ul style="list-style-type: none"> <li>Nivel de satisfacción de los interesados con el conocimiento y la cualificación del personal</li> <li>Porcentaje de personal cuya cualificación es insuficiente para la competencia requerida por su rol</li> <li>Porcentaje de personal satisfecho</li> </ul>
	17. Cultura de innovación de producto y negocio	<ul style="list-style-type: none"> <li>Nivel de concienciación y comprensión de las oportunidades de innovación del negocio</li> <li>Satisfacción de los interesados con los niveles de conocimiento e ideas de innovación y productos</li> <li>Número de iniciativas de productos y servicios aprobadas resultantes de ideas innovadoras</li> </ul>

Ilustración 22. Muestra de Métricas de Metas Corporativas

(COBIT 5 – Procesos Catalizadores)

En la cuarta figura, mostrada a continuación, podemos ver ejemplos de métricas de metas TI. La información se divide en dimensión del CMI, objetivos de las TI y métrica.

Dimensión CMI	Objetivos de las TI	Métrica
Financiera	01 Alineamiento de TI y estrategia de negocio	<ul style="list-style-type: none"> <li>Porcentaje de metas estratégicas y requerimientos corporativos apoyados por metas TI estratégicas</li> <li>Nivel de satisfacción de los interesados con el alcance del portfolio de programas y servicios planificado</li> <li>Porcentaje de factores de valor TI mapeados a factores de valor del negocio</li> </ul>
	02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	<ul style="list-style-type: none"> <li>Coste de incumplimientos TI, incluyendo acuerdos y sanciones e impacto en pérdida de reputación</li> <li>Número de incumplimientos TI reportados al Consejo de Administración o causantes de comentarios o vergüenza públicos</li> <li>Número de incumplimientos relacionados con proveedores de servicios TI</li> <li>Cobertura de evaluaciones de cumplimiento</li> </ul>
	03 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	<ul style="list-style-type: none"> <li>Porcentaje de roles de la dirección ejecutiva con responsabilidad claramente definida en decisiones TI</li> <li>Número de veces que TI está en la agenda del Consejo de Administración de manera proactiva</li> <li>Frecuencia de reuniones del comité ejecutivo de estrategia de TI</li> <li>Tasa de ejecución de decisiones TI ejecutivas</li> </ul>
	04 Riesgos de negocio relacionados con las TI gestionados	<ul style="list-style-type: none"> <li>Porcentaje de procesos TI de negocio críticos, servicios TI y programas de negocio habilitados por TI cubiertos por evaluaciones de riesgo</li> <li>Número de incidentes TI significativos que no fueron identificados en evaluaciones de riesgos</li> <li>Porcentaje de evaluaciones de riesgo corporativas que incluyen riesgo TI</li> <li>Frecuencia de actualización del perfil de riesgo</li> </ul>

Dimensión CMI	Objetivos de las TI	Métrica
Financiera (cont.)	05 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	<ul style="list-style-type: none"> <li>• Porcentaje de inversiones TI donde la obtención del beneficio se supervisa a lo largo de todo el ciclo de vida económico</li> <li>• Porcentaje de servicios TI donde se obtienen los beneficios esperados</li> <li>• Porcentaje de inversiones TI donde se cumplen o exceden los beneficios esperados</li> </ul>
	06 Transparencia de los costes, beneficios y riesgos de las TI	<ul style="list-style-type: none"> <li>• Porcentaje de casos de negocio de inversiones TI con costes TI y beneficios esperados claramente definidos y aprobados</li> <li>• Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados</li> <li>• Encuesta de satisfacción de interesados clave en relación con el nivel de transparencia, comprensión y precisión de información financiera TI</li> </ul>
Cliente	07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	<ul style="list-style-type: none"> <li>• Número de interrupciones de negocio debidas a incidentes de servicios TI</li> <li>• Porcentaje de partes interesadas en el negocio satisfechas de que la entrega de servicios TI cumpla los niveles de servicio acordados</li> <li>• Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios TI</li> </ul>
	08 Uso adecuado de aplicaciones, información y soluciones tecnológicas	<ul style="list-style-type: none"> <li>• Porcentaje de propietarios de procesos de negocio satisfechos con el apoyo de productos y servicios TI</li> <li>• Nivel de entendimiento de los usuarios del negocio sobre cómo las soluciones tecnológicas apoyan sus procesos</li> <li>• Nivel de satisfacción de los usuarios de negocio con la formación y los manuales de usuario</li> <li>• Valor presente neto (NPV) mostrando el nivel de satisfacción del negocio con la calidad y utilidad de las soluciones tecnológicas</li> </ul>
Interno	09 Agilidad de las TI	<ul style="list-style-type: none"> <li>• Nivel de satisfacción de la alta dirección del negocio con la capacidad de respuesta de TI a nuevos requerimientos</li> <li>• Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas</li> <li>• Tiempo medio de conversión de objetivos TI estratégicos en una iniciativa acordada y aprobada</li> </ul>
	10 Seguridad de la información, infraestructuras de procesamiento y aplicaciones	<ul style="list-style-type: none"> <li>• Número de incidentes de seguridad causantes de pérdidas financieras, interrupción del negocio o vergüenza pública</li> <li>• Número de servicios TI sin requerimientos de seguridad destacables</li> <li>• Tiempo de concesión, cambio y eliminación de privilegios de acceso comparado con los niveles de servicio acordados</li> <li>• Frecuencia de las evaluaciones de seguridad en relación a los últimos estándares y guías</li> </ul>
	11 Optimización de activos, recursos y capacidades de las TI	<ul style="list-style-type: none"> <li>• Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes</li> <li>• Tendencia de los resultados de las evaluaciones</li> <li>• Niveles de satisfacción de la alta dirección del negocio y de TI con los costes y capacidades TI</li> </ul>
	12 Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	<ul style="list-style-type: none"> <li>• Número de incidentes del procesamiento de negocio causados por errores de integración de la tecnología</li> <li>• Número de cambios en los procesos de negocio que tienen que ser retrasados o revisados debido a problemas de integración de la tecnología</li> <li>• Número de programas de negocio facilitados por TI retrasados o incurriendo en costes adicionales debido a problemas de integración de la tecnología</li> <li>• Número de aplicaciones o infraestructuras críticas operando aisladamente y no integradas</li> </ul>
	13 Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	<ul style="list-style-type: none"> <li>• Número de programas/proyectos en tiempo y en presupuesto</li> <li>• Porcentaje de interesados satisfechos con la calidad del programa/proyecto</li> <li>• Número de programas que necesitan revisiones significativas debido a defectos de calidad</li> <li>• Coste de mantenimiento de las aplicaciones respecto al coste TI global</li> </ul>
	14 Disponibilidad de información útil y relevante para la toma de decisiones	<ul style="list-style-type: none"> <li>• Nivel de satisfacción del usuario del negocio con la calidad y la puntualidad (o disponibilidad) de la información de gestión</li> <li>• Número de incidentes de procesos de negocio causados por la indisponibilidad de la información</li> <li>• Relación y alcance de decisiones de negocio erróneas donde la información errónea o no disponible fue un factor clave</li> </ul>
	15 Cumplimiento de las políticas internas por parte de las TI	<ul style="list-style-type: none"> <li>• Número de incidentes relacionados con el incumplimiento de políticas</li> <li>• Porcentaje de interesados que entienden las políticas</li> <li>• Porcentaje de políticas apoyadas por estándares y prácticas de trabajo efectivas</li> <li>• Frecuencia de revisión y actualización de políticas</li> </ul>
Aprendizaje y Crecimiento	16 Personal del negocio y de las TI competente y motivado	<ul style="list-style-type: none"> <li>• Porcentaje de personal cuyas habilidades TI son suficientes para la competencia requerida por sus roles</li> <li>• Porcentaje de personal satisfecho con sus roles en TI</li> <li>• Número de horas de aprendizaje/ formación por miembro del personal</li> </ul>
	17 Conocimiento, experiencia e iniciativas para la innovación de negocio	<ul style="list-style-type: none"> <li>• Nivel de concienciación y comprensión de la alta dirección del negocio sobre las posibilidades de innovación TI</li> <li>• Nivel de satisfacción de los interesados con los niveles de experiencia e ideas de innovación de TI</li> <li>• Número de iniciativas aprobadas resultantes de ideas TI innovadoras</li> </ul>

Ilustración 23. Ejemplo de Métricas de Metas TI

(COBIT 5 – Procesos Catalizadores)

En la quinta figura, mostrada a continuación, se puede ver el mapeo entre las necesidades de las partes interesadas y las metas corporativas, que sería el paso en cascada entre necesidades de las partes interesadas y metas corporativas que se puede ver en la Ilustración 3.

NECESIDADES DE LAS PARTES INTERESADAS	Valor para los interesados de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basada en información	Optimización de los costes de los procesos de negocio	Optimización de la funcionalidad de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Cumplimiento con políticas internas	Personas preparadas y motivadas	Cultura de innovación de producto y negocio
	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
¿Cómo se consigue valor mediante el uso de TI? ¿Está el usuario final satisfecho con la calidad del servicio de TI?																	
¿Cómo se gestiona el rendimiento de TI?																	
¿Cómo se puede explotar mejor la tecnología de red para conseguir nuevas oportunidades estratégicas?																	
¿Cómo puedo construir y estructurar mejor mi departamento de TI?																	
¿Cuánto dependo de mis proveedores externos? ¿Cómo de bien están siendo gestionados los acuerdos de externalización de TI? ¿Cómo puedo verificarlos sobre proveedores externos?																	
¿Cuáles son los requisitos (de control) para la información?																	
¿He contemplado todo los riesgos relacionados con TI?																	
¿Estoy ejecutando una operación de TI eficiente y robusta?																	
¿Cómo se controla el coste de TI? ¿Cómo se usan los recursos de TI en la manera más efectiva y eficiente? ¿Cuáles son las opciones de aprovisionamiento más efectivas y eficientes?																	



NECESIDADES DE LAS PARTES INTERESADAS	Valor para los Interesados de las Inversiones de Negocio	Carta de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basada en Información	Optimización de los costes de los procesos de negocio	Optimización de la funcionalidad de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Cumplimiento con políticas internas	Personas preparadas y motivadas	Cultura de innovación de producto y negocio
	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
¿Tengo suficiente personal para TI? ¿Cómo puedo desarrollar y mantener sus habilidades y cómo gestiono su rendimiento?																	
¿Cómo consigo confianza sobre TI?																	
¿Está bien securizada la información que se está procesando?																	
¿Cómo se puede mejorar la capacidad de respuesta del negocio mediante un entorno de IT más flexible?																	
¿Fracasan los proyectos de TI en proporcionar lo que habían prometido? Si es así, ¿por qué permanece la TI en el camino de ejecutar la estrategia de negocio?																	
¿Cómo es de crítica la TI para para la sostenibilidad de la empresa? ¿Qué pasaría si la TI no estuviera disponible?																	
¿Qué procesos de negocio críticos dependen de TI y cuáles son los requerimientos de los procesos de negocio?																	
¿En cuánto han excedido de media los presupuestos de operación de TI? ¿Con qué frecuencia y cuánto se salen del presupuesto los proyectos de TI?																	
¿Qué parte del esfuerzo de TI se dedica a apagar fuegos en lugar de facilitar las mejoras del negocio?																	
¿Son suficientes los recursos y la infraestructura de TI disponibles para conseguir los objetivos estratégicos de empresa requeridos?																	
¿Cuánto se tarda en la toma de decisiones importantes de TI?																	
¿Son transparentes el esfuerzo y las inversiones totales en TI?																	
¿Respalda TI a la empresa en el cumplimiento de la normativa y los niveles de servicio? ¿Cómo puedo saber si se cumple con todas las normas aplicables?																	

Ilustración 24. Mapeo entre las Metas Corporativas y las Preguntas del Gobierno y la Gestión

(COBIT 5 – Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa)

En la sexta figura, mostrada a continuación, se puede ver el mapeo entre las metas corporativas y las metas TI, que sería el paso en cascada entre metas corporativas y metas TI que se puede ver en la Ilustración 3.

			Objetivo Corporativo																
			Valor para las partes interesadas de las inversiones de negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activo)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basadas en información	Optimización de costos de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costos de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personal entrenado y motivado	Cultura de innovación del producto y del negocio
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
Objetivo Relativo a TI			Financiera					Cliente					Interna					Aprendizaje y Crecimiento	
Financiera	01	Alineamiento de TI y la estrategia de negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P		
	03	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	04	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	05	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	06	Transparencia de los costes, beneficios y riesgos de las TI	S		S		P				S	P		P					
Cliente	07	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interna	09	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructuras de procesamiento y aplicaciones			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de las políticas internas por parte de las TI			S	S											P		
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S					P			P	S
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S		S		S			S	P

Ilustración 25. Mapeo entre las Metas Corporativas y Metas TI

En la séptima figura, mostrada a continuación, se puede ver el mapeo entre las metas TI y los procesos, que sería el paso en cascada entre metas TI y catalizadores que se puede ver en la Ilustración 3.

			Meta relacionada con las TI																
			Alineamiento de TI y la estrategia de negocio																
			Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas																
			Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI																
			Riesgos de negocio relacionados con las TI gestionados																
			Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI																
			Transparencia de los costos, beneficios y riesgos de las TI																
			Entrega de servicios de TI de acuerdo a los requisitos del negocio																
			Uso adecuado de aplicaciones, información y soluciones tecnológicas																
			Agilidad de las TI																
			Seguridad de la información, infraestructura de procesamiento y aplicaciones																
			Optimización de activos, recursos y capacidades de las TI																
			Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio																
			Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.																
			Disponibilidad de información útil y relevante para la toma de decisiones																
			Cumplimiento de las políticas internas por parte de las TI																
			Personal del negocio y de las TI competente y motivado																
			Conocimiento, experiencia e iniciativas para la innovación de negocio																
Procesos de COBIT 5			Financiera					Cliente			Interna							Aprendizaje y Crecimiento	
Evaluar, Orientar y Supervisar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Asegurar la Entrega de Beneficios	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Asegurar la Optimización del Riesgo	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Asegurar la Optimización de los Recursos	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Asegurar la Transparencia hacia las partes interesadas	S	S	P			P	P						S	S	S		S
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI	P	P	S	S		S		P	S	P	S	S	S	S	P	P	P
	APO02	Gestionar la Estrategia	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Gestionar la Arquitectura Empresarial	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Gestionar la Innovación	S			S	P			P	P		P	S		S			P
	APO05	Gestionar el portafolio	P		S	S	P	S	S	S	S		S		P				S
	APO06	Gestionar el Presupuesto y los Costes	S		S	S	P	P	S	S			S		S				
	APO07	Gestionar los Recursos Humanos	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Gestionar las Relaciones	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Gestionar los Acuerdos de Servicio	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	Gestionar los Proveedores		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	Gestionar la Calidad	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	Gestionar el Riesgo		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	Gestionar la Seguridad		P		P		P	S	S		P				P			



			Meta relacionada con las TI																
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costos, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Procesos de COBIT 5			Financiera					Cliente			Interna							Aprendizaje y Crecimiento	
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Gestionar la Definición de Requisitos	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Gestionar la Identificación y la Construcción de Soluciones	S			S	S		P	S			S	S	S	S			S
	BAI04	Gestionar la Disponibilidad y la Capacidad				S	S		P	S	S		P		S	P			S
	BAI05	Gestionar la introducción de Cambios Organizativos	S		S		S		S	P	S		S	S	P				P
	BAI06	Gestionar los Cambios			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Gestionar la Aceptación del Cambio y de la Transición				S	S		S	P	S			P	S	S	S		S
	BAI08	Gestionar el Conocimiento	S				S		S	S	P	S	S			S		S	P
	BAI09	Gestionar los Activos		S		S		P	S		S	S	P			S	S		
	BAI10	Gestionar la Configuración		P		S		S		S	S	S	P			P	S		
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio				P			P	S		S				S	S		S
	DSS03	Gestionar los Problemas		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Gestionar la Continuidad	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Gestionar los Servicios de Seguridad	S	P		P			S	S		P	S	S		S	S		
	DSS06	Gestionar los Controles de los Procesos del Negocio		S		P			P	S		S	S	S		S	S	S	S
Supervisión, Evaluación y Verificación	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno		P		P		S	S	S		S				S	P		S
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		P		P	S		S			S					S		S

Ilustración 26. Mapeo entre las Metas Relacionadas con la TI y los Procesos

(COBIT 5 – Procesos Catalizadores)

## Apéndice II

El primer cuestionario que vamos a realizar es el correspondiente al área de planificación que se divide en las preguntas correspondientes a sistemas de información, a recursos humanos y a otros aspectos correspondientes al área de planificación, teniendo como objetivo sondear la planeación que se realizó para formar el área de sistemas, siendo de vital importancia para el desempeño del área, pues verifica si los objetivos y los alcances del área corresponden a los desempeñados.

### Cuestionario de Auditoría correspondiente al área de planificación:

#### 1. Sistemas de información

1.1 ¿La dirección general y ejecutiva ha considerado la importancia que tiene el estudio del sistema de información? SI ( ) NO ( x )

1.2 ¿Se establecen los requisitos de información a largo plazo? SI ( ) NO ( x )

1.3 ¿Se ha realizado una planificación estratégica del sistema de información para la Empresa? SI ( ) NO ( x )

1.4 ¿Existe una metodología para llevar a cabo tal planificación? SI ( ) NO ( x )

1.5 ¿Está definida la función del director del sistema de información? SI ( x ) NO ( )

1.6 ¿Existe un plan estratégico del departamento de sistema de información?  
SI ( x ) NO ( )

#### 2. Recursos humanos

2.1 ¿Se estudia la evolución del mercado y la adaptación del personal a esa evolución? SI ( ) NO ( x )

2.2 ¿Los informáticos reciben noticias del momento tecnológico por revistas, notas técnicas, etc.? SI ( x ) NO ( )

2.3 ¿Se recibe formación y se planifica ésta mediante asistencia a cursos, seminarios, etc.? SI ( x ) NO ( )

#### 3. Otros aspectos

3.1 ¿Los cambios en los sistemas informáticos son consecuencia de la planificación más que de la presión por necesidades operativas? SI ( ) NO ( x )

3.2 ¿Se solicitan demostraciones sobre los nuevos artículos a los proveedores?  
SI ( x ) NO ( )

3.3 ¿Se ha realizado algún estudio de planificación del posible efecto de las cargas normales de trabajo y los picos sobre los requerimientos tanto de equipos como de software? SI ( x ) NO ( )

3.4 ¿La entidad dispone de un plan informático? SI ( x ) NO ( )

3.5 ¿Se están siguiendo las directrices marcadas por el plan? SI ( x ) NO ( )

3.6 ¿El plan recoge todos los diferentes aspectos relacionados con la función informática? SI ( x ) NO ( )

3.7 ¿Cuál es la inversión requerida en servicios, desarrollo y consulta a los usuarios? 95% jornada

El segundo cuestionario es el correspondiente a los dispositivos de almacenamiento y este cuestionario tiene como objetivo evaluar la administración, la aplicación y el uso de dispositivos, hardware, de almacenamiento de información electrónico de la organización.

#### **Cuestionario de Auditoría correspondiente a los dispositivos de almacenamiento:**

1. Los locales asignados a los servidores de datos tienen

- Aire acondicionado ( x )
- Protección contra el fuego ( x )
- Cerradura especial ( x )
- Otra:

2. ¿Tienen los servidores de datos protección automática contra el fuego?

SI ( ) NO ( x )

(Señalar de que tipo)

3. ¿Que información mínima contiene el inventario de los servidores de datos?

- Número de serie o carrete ( x )
- Número o clave del usuario ( )
- Número del archivo lógico ( )
- Nombre del sistema que lo genera ( )
- Fecha de expiración del archivo ( )
- Número de volumen ( )
- Otros

4. ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?

SI ( ) NO ( x )

5. ¿En caso de existir discrepancia entre las cintas o discos y su contenido, se resuelven y explican satisfactoriamente las discrepancias? SI ( x ) NO ( )

6. ¿Se tienen procedimientos que permitan la reconstrucción de un archivo en cinta a disco, el cual fue inadvertidamente destruido? SI ( ) NO ( x )

7. ¿Se tienen identificados los archivos con información confidencial y se cuenta con claves de acceso? SI ( x ) NO ( )

¿Cómo se tienen identificados los archivos con información confidencial?

Por carpetas en servidor y protegidas por permisos de usuario

¿Con que tipo de claves de acceso se cuenta?

Dos niveles, acceso al equipo y acceso a la carpeta por usuario, letras, caracteres y numérica

8. ¿Existe un control estricto de las copias de estos archivos? SI ( x ) NO ( )

9. ¿Que medio se utiliza para almacenarlos?

Mueble con cerradura ( x )

Bóveda ( )

Otro (especifique):

10. Este almacén está situado:

En el mismo edificio del departamento ( )

En otro lugar ( x ) ¿Cual?:

Otra sede

11. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos? SI ( x ) NO ( )

12. ¿Se certifica la destrucción o baja de los archivos defectuosos? SI ( x ) NO ( )

13. ¿Se registran como parte del inventario las nuevas cintas que recibe la biblioteca?

SI ( x ) NO ( )

14. ¿Se tiene un responsable, por turno, de los servidores de datos? SI ( ) NO ( x )

15. ¿Se realizan auditorías periódicas a los medios de almacenamiento? SI ( ) NO ( x )

16. ¿Qué medidas se toman en el caso de extravío de algún dispositivo de almacenamiento?

Los dispositivos de almacenamiento están encriptados con una clave de 256 caracteres

17. ¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado? SI ( x ) NO ( )

18. ¿Se tiene relación del personal autorizado para firmar la salida de archivos confidenciales? SI ( x ) NO ( )

19. ¿Existe un procedimiento para registrar los archivos que se prestan y la fecha en que se devolverán? SI (x ) NO ( )

20. ¿Se lleva control sobre los archivos prestados por la instalación? SI ( ) NO ( x )

21. En caso de préstamo ¿Con que información se documentan?

Nombre de la institución a quién se hace el préstamo.

Fecha de recepción ( )

Fecha en que se debe devolver ( )

Archivos que contiene

Formatos

Cifras de control ( )

Código de grabación ( )

Nombre del responsable que los preste

Otros

22. Indique qué procedimiento se sigue en el reemplazo de las cintas que contienen los archivos maestros:

23. ¿Se conserva la cinta maestra anterior hasta después de la nueva cinta?

SI ( ) NO (x )

24. ¿La operación de reemplazo es controlada por el operador? SI ( ) NO ( x )

25. En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperar los archivos? SI ( ) NO (x )

26. ¿Estos procedimientos para recuperar los archivos los conocen los operadores?

SI ( ) NO ( x )

27. ¿Con que periodicidad se revisan estos procedimientos?

MENSUAL ( )

ANUAL ( )

SEMESTRAL ( )

OTRA ( ):

28. ¿Existe un responsable en caso de falla? SI ( ) NO (x)

29. ¿Existe un procedimiento para el manejo de la información del *cuarto frío*?

SI ( ) NO (x)

30. ¿El procedimiento para el manejo de la información del cuarto frío lo conoce y lo sigue el operador?

SI ( ) NO (x)

31. ¿Se distribuyen en forma periódica entre los jefes de sistemas y programación informes de archivos para que liberen los dispositivos de almacenamiento?

SI ( ) NO (x) ¿Con qué frecuencia?:

--

El tercer cuestionario es el correspondiente al funcionamiento del centro de cómputo y este cuestionario tiene como objetivo evaluar el correcto funcionamiento, así como la organización del centro de cómputo, tomando en cuenta los reglamentos del área. Así como también revisar que estos reglamentos tengan como objetivo mantener el orden del centro de cómputo.

#### **Cuestionario de Auditoría correspondiente al funcionamiento del centro de cómputo:**

1. ¿El lugar donde se ubica el centro de cómputo está seguro de inundaciones, robo o cualquier otra situación que pueda poner en peligro los equipos? SI (x) NO ( )

2. ¿El centro de cómputo da hacia el exterior? SI ( ) NO (x)

3. ¿El material con que está construido el centro de cómputo es confiable?

SI ( ) NO (x)

4. ¿Dentro del centro de cómputo existen materiales que puedan ser inflamables o causar algún daño a los equipos? SI ( ) NO (x) ¿Cuál?:

--

5. ¿Existe lugar suficiente para los equipos? SI ( ) NO (x)

6. ¿Aparte del centro de cómputo se cuenta con algún lugar para almacenar otros equipos de cómputo, muebles, suministros, etc.? SI (x) NO ( ) ¿Dónde?:

En cada sede
--------------

7. ¿Se cuenta con una salida de emergencia? SI (x) NO ( )

8. ¿Existen señalamientos que hagan visibles las salidas de emergencia?

SI ( x ) NO ( ) ¿Dónde?:

En los lugares adecuados, en cada sede hay un plan de evacuación

9. ¿Es suficiente la iluminación del centro de cómputo? SI (x) NO ( ) ¿Por qué?:

Por las luces que hay

10. ¿La temperatura a la que trabajan los equipos es la adecuada de acuerdo a las normas bajo las cuales se rige? SI ( ) NO ( x )

11. ¿Se dispone de aire acondicionado? SI ( ) NO ( x )

12. ¿La ubicación de los aires acondicionado es adecuada? SI ( ) NO ( )

13. ¿Existe algún otro medio de ventilación aparte del aire acondicionado?

SI ( x ) NO ( ) ¿Cuál?:

Ventanas y rejillas

14. ¿El aire acondicionado emite algún tipo de ruido? SI (x) NO ( )

15. ¿El cableado se encuentra correctamente instalado? SI ( x ) NO ( )

16. ¿Se cuenta con los planos de instalación eléctrica? SI (x) NO ( )

17. ¿La instalación eléctrica del equipo de cómputo es independiente de otras instalaciones? SI ( ) NO ( x )

18. ¿Los equipos cuentan con un regulador? SI ( ) NO ( x )

19. ¿Se cuenta con equipo interrumpible? SI ( ) NO ( x )

20. ¿Se tiene switch de apagado en caso de emergencia en algún lugar visible?

SI ( ) NO (x )

21. ¿Los cables están dentro de paneles y canales eléctricos? SI ( x ) NO ( )

22. ¿Los interruptores de energía están debidamente protegidos y sin obstáculos para alcanzarlos? SI ( x ) NO ( )

23. ¿Se cuenta con alarma contra incendios? SI ( x ) NO ( )

24. ¿Dónde se encuentran ubicadas las alarmas contra incendios?

En las sedes, son comunes.

25. ¿Se cuenta con alarmas contra inundaciones? SI ( ) NO ( x )

26. ¿Dónde se encuentran ubicadas las alarmas contra inundaciones?

27. ¿Existen extintores? SI ( x ) ¿Cuántos?: 1 por cada sede, 25 NO ( )

Tipos de extintores: Manual ( x ) Automático ( ) No existen ( )

28. ¿Hay algún tipo de control de entradas y salidas de usuario? SI ( ) NO ( x )

29. ¿El usuario respeta el control de entradas y salidas de usuario? SI ( ) NO ( )

30. ¿Con que tipo de programas cuentan en los equipos de cómputo?

No disponemos de equipos de cómputo

31. ¿Cuentan con manuales para cada programa que se maneja? SI ( ) NO ( x )

32. ¿El personal sabe del contenido de estos manuales para cada programa?

SI ( ) NO ( x )

33. ¿Qué tipo de mantenimiento realizan de los programas?

A. Preventivo ( ) B. Correctivo ( x )

34. ¿Por qué razón realizan ese tipo de mantenimiento?

No disponemos de tiempo para hacer el preventivo y sólo mantenemos y corregimos necesidades detectadas.

35. ¿Qué materiales utilizan para realizar el mantenimiento del hardware?

Compresor para limpieza

36. ¿Tienen un lugar específico para guardar el material de mantenimiento de hardware? SI ( x ) NO ( )

37. ¿Qué materiales utilizan para realizar el mantenimiento de software?

No disponemos

38. ¿Tienen un lugar específico para guardar el material de mantenimiento de software? SI ( x ) NO ( )

39. ¿Los usuarios tienen la suficiente confianza como para presentar su queja si fallasen los equipos? SI ( x ) NO ( )

40. ¿Se efectúan controles o revisiones del buen estado de los equipos de cómputo?

SI ( x ) NO ( )

41. ¿Las inspecciones son realizadas por personal especializado como técnicos o mecánicos electrónicos? SI ( x ) NO ( )

42. ¿Los datos de clientes y proveedores se salvaguardan por parte del sistema?

SI ( x ) NO ( )



43. ¿Se implementan medidas de seguridad en los computadores de los empleados para evitar que estos ejecuten programas peligrosos? SI ( x ) NO ( )
44. ¿Existe un programa de protección de la información contra virus, spyware y diferentes ataques cibernéticos? SI ( x ) NO ( )
45. ¿Se usan claves para acceder a las bases de datos? SI ( x ) NO ( )
46. ¿Todos los empleados pueden acceder a estas? SI ( ) NO ( x )

El cuarto cuestionario es el correspondiente a la seguridad física y este cuestionario verifica la seguridad física de las instalaciones que utiliza el área de sistemas, ya que de esto depende la continuidad de los servicios que presta el área a la organización, en cuanto a necesidades de información.

#### **Cuestionario de Auditoría correspondiente a la seguridad física:**

1. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información? SI ( ) NO ( x )
2. ¿Existen una persona responsable de la seguridad? SI ( ) NO ( x )
3. ¿Existe personal de vigilancia en la institución? SI ( ) NO ( x )
4. ¿La vigilancia se contrata?  
Directamente ( )  
Por medio de empresas que venden ese servicio ( )
5. ¿Existe una clara definición de funciones entre los puestos clave? SI ( ) NO ( x )
6. ¿Se investiga a los vigilantes cuando son contratados directamente? SI ( ) NO ( x )
7. ¿Se controla el trabajo fuera de horario? SI ( ) NO ( x )
8. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas? SI ( ) NO ( x )
9. ¿Existe vigilancia en el departamento de cómputo las 24 horas? SI ( ) NO ( x )
10. ¿Existe vigilancia a la entrada del departamento de cómputo las 24 horas?  
Vigilante ( )  
Recepcionista ( )  
Tarjeta de control de acceso ( )  
Nadie ( x )
11. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores? SI ( x ) NO ( )
12. ¿Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización? SI ( ) NO ( x )

13. El edificio donde se encuentra la computadora está situado a salvo de:

Inundación ( )

Terremoto ( )

Fuego ( )

Sabotaje ( )

Nada (x)

14. Describa brevemente la construcción del centro de cómputo, de preferencia proporcionando planos y material con que construirlo y equipo (muebles, sillas, etc.) dentro del centro.

No disponemos de espacio

15. ¿Existe control en el acceso a este cuarto?

Por identificación personal ( )

Por tarjeta magnética ( )

Por claves verbales ( )

Otras ( )

16. ¿Son controladas las visitas y demostraciones en el centro de cómputo?

SI ( ) NO (x)

17. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática? SI ( ) NO (x)

18. Existe alarma en las instalaciones para:

Detectar fuego (calor o humo) de forma automática (x)

Avisar en forma manual la presencia del fuego ( )

Detectar una fuga de agua ( )

Detectar magnéticos ( )

No existe ( )

19. Estas alarmas están:

En el departamento de cómputo ( )

En el cuarto frío ( )

No están (x)

Otros:

20. ¿Existe alarma para detectar condiciones anormales del ambiente?

En el departamento de cómputo ( )

En el cuarto frío ( )

En otros lados:

No existe

21. ¿La alarma es perfectamente audible? SI ( ) NO ( x )

22. Esta alarma también está conectada:

Al puesto de guardias ( )

A la estación de bomberos ( )

A ningún otro lado ( )

Otros:

No disponemos

23. Existen extintores de fuego

Manuales ( x )

Automáticos ( )

No existen ( )

24. ¿Se ha adiestrado el personal en el manejo de los extintores? SI ( x ) NO ( )

25. Los extintores, manuales o automáticos a base de

Agua ( )

Gas ( )

Otros ( x , no disponemos)

26. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?

SI ( x ) NO ( )

27. ¿Si es que existen extintores automáticos son activados por detectores automáticos de fuego? SI ( ) NO ( )

28. Si los extintores automáticos son a base de agua, ¿se han tomado medidas para evitar que el agua cause más daño que el fuego? SI ( ) NO ( )

29. ¿Si los extintores automáticos son a base de gas, ¿se ha tomado medidas para evitar que el gas cause más daño que el fuego? SI ( ) NO ( )

30. Existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos para que el personal:

¿Corte la acción de los extintores por tratarse de falsas alarmas? SI ( ) NO ( )

¿Pueda cortar la energía eléctrica? SI ( ) NO ( )

¿Pueda abandonar el local sin peligro de intoxicación? SI ( ) NO ( )

- ¿Es inmediata su acción? SI ( ) NO ( )
31. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos? SI ( ) NO ( x )
32. ¿Existe salida de emergencia? SI ( x ) NO ( )
33. Esta puerta solo es posible abrirla:
- ¿Desde el interior? ( )
  - ¿Desde el exterior? ( )
  - Ambos lados ( x )
34. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen? SI ( x ) NO ( )
35. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia? SI ( x ) NO ( )
36. Se ha tomado medidas para minimizar la posibilidad de fuego:
- Evitando artículos inflamables en el departamento de cómputo ( x )
  - Prohibiendo fumar a los operadores en el interior ( x )
  - Vigilando y manteniendo el sistema eléctrico ( x )
  - No se ha previsto ( )
37. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo? SI ( x ) NO ( )
38. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?
- SI ( x ) NO ( )
39. ¿Cuándo se efectúan modificaciones a los programas, a iniciativa de quién es?
- Usuario ( x )
  - Director de informática ( x )
  - Jefe de análisis y programación ( )
  - Programador ( x )
  - Otras (especifique):
- 
40. Las solicitudes de modificaciones a los programas se hacen en forma:
- Oral ( )
  - Escrita ( x )
41. Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?
- SI ( x ) NO ( )
42. ¿Existe control estricto en las modificaciones? SI ( x ) NO ( )

43. ¿Si se tienen terminales conectadas, ¿se ha establecido procedimientos de operación? SI ( x ) NO ( )

44. Se verifica identificación:

De la terminal ( x )

Del usuario (x )

No se pide identificación ( )

45. ¿Se ha establecido un número máximo de violaciones en sucesión para que la computadora cierre esta terminal y se de aviso al responsable de ella? SI ( ) NO ( x )

46. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones? ¿Cuáles son?

( x ) Recepción de documentos

Plantilla de recepción

( ) Información confidencial

( ) Captación de documentos

( ) Cómputo electrónico

( ) Programas

( x ) Documentos de salida

Plantilla de salida de documentos

( ) Archivos magnéticos

( ) Operación del equipo de computación

( ) En cuanto al acceso de personal

( ) Identificación del personal

( ) Policía

( x) Seguros contra robo e incendio

Póliza contenido contingente

( ) Cajas de seguridad

( ) Otras (especifique)